Universidad
Carlos III de Madrid

TRABAJO FIN DE GRADO

Gestión de Métricas de Seguridad sobre Proveedores de Servicios Cloud

Autor: José Romero Candía

Tutoras: Florina Almenares Mendoza
Patricia Arias Cabarcos

Leganés, septiembre de 2015

Título: Gestión de métricas de seguridad sobre proveedores de servicios cloud
Autor: José Romero Candía
Directores: Florina Almenares Mendoza, Patricia Arias Cabarcos

EL TRIBUNAL

Presidente: _____

Vocal: _____

Secretario: _____

Realizado el acto de defensa y lectura del Proyecto Fin de Carrera el día 15 de octubre de 2015 en Leganés, en la Escuela Politécnica Superior de la Universidad Carlos III de Madrid, acuerda otorgarle la CALIFICACIÓN de

VOCAL

SECRETARIO PRESIDENTE

Agradecimientos

A mis tutoras, Florina y Patricia, por toda su implicación e interés en este proyecto y por su ayuda que nunca faltó cuando la necesitaba.

A mis compañeros de clase, por hacer más llevaderos estos cuatro años de carrera y, espero, que los siguientes de Máster.

A mi familia y amigos, por su apoyo presente tanto en el desarrollo de este proyecto como a lo largo de la carrera que me ha dado fuerzas para llegar hasta el final.

Resumen

El mundo de las Tecnologías de Información y Comunicación (TIC) se encuentra en un proceso de evolución constante. Una de las tendencias actuales es el uso de servicios de *Cloud Computing*, también conocido como la "Nube". Estos servicios proporcionan el acceso bajo demanda a recursos, como herramientas software, servidores o sistemas de almacenamiento, y que supone una gran reducción de costes de infraestructura para los clientes.

Sin embargo, existe cierta desconfianza acerca de los riesgos que conlleva contratar servicios *Cloud*. Las preocupaciones provienen de temas como la confidencialidad de los datos y su gestión, especialmente con información sensible, o la pérdida de datos. Por ello, la seguridad es un aspecto clave.

El objetivo principal de este Proyecto Fin de Grado consiste precisamente en desarrollar una herramienta que permita procesar la información disponible sobre las métricas de seguridad de los proveedores de servicios de *Cloud Computing*, y hacerla disponible a través de un servicio Web. De esta manera, los usuarios pueden evaluar los servicios proporcionados por diferentes proveedores y compararlos para obtener el servicio que más se ajuste a sus necesidades.

En particular, este proyecto se centra el desarrollo de un sistema que permita a otras aplicaciones acceder a los metadatos basados en métricas de seguridad, a través de una API. Dichos metadatos son obtenidos mediante el procesamiento de documentos de validación de servicios Cloud (CAIQ) proporcionados por la *Cloud Security Alliance* (CSA).

Palabras clave: *Cloud Computing*, seguridad, proveedores, evaluación de servicios Cloud, métricas de seguridad, CAIQ, servicio Web, API, *Cloud Security Alliance*.

Abstract

Information and Communications Technologies (ICT) are constantly evolving. One of the current trends is the use of Cloud Computing services. These services provide on-demand access to resources such as software tools, servers and storage systems, by representing a reduction of infrastructure costs for customers.

However, there is some distrust about the risks of contracting cloud services. The concern stems from privacy management, especially with sensitive information, or data loss; therefore, security is a key point.

The main objective of this Final Degree Project is precisely the development of a tool that processes the available information about security metrics of Cloud Computing service providers, and that makes it accessible through a Web service. In this way, users can assess services of different providers and compare them to get the service that best suits their needs.

In particular, this project is focused on developing a system that allows other applications to access a security metrics based on providers' metadata through a Web service. This metadata is obtained by processing cloud service assessment documents (CAIQ) provided by the Cloud Security Alliance (CSA).

Keywords: Cloud Computing, security, cloud providers, cloud service assessment, security metrics, CAIQ, Web service, API, Cloud Security Alliance.

Índice general

Índice de figuras

Índice de tablas

1 Introduction

1.1 Context and motivation

In recent years, there has been an increase in computing needs of companies that cannot be satisfied by the capacity of current equipment and personal computers, due to the development of ICT (Information and Communication Technologies). This need from enterprises, together with the evolution of technologies in the field of distributed computing and absolute presence of Internet in our lives, has led to a current trend called *Cloud Computing* or simply *Cloud*.

The cloud model provides high computing and storage capabilities to enterprises and organizations without needing to own infrastructure. *Cloud Computing* also provides tools and applications on demand. The most important features of cloud services are resources scalability and the abstraction of underlying technologies for customers. As a result, the current trend for companies is to adopt cloud computing solutions.

However, the use of cloud entails risks and threats, so it is very important to analyse the security of these services. There are organizations such as Cloud Security Alliance (CSA), which promotes the use of best practices for securing cloud computing and provides security education and guidance to companies. These practices include the assessment of the risk of contracting a cloud service provider (CSP) or the analysis of the security requirements based on company needs.

CSA provides a useful tool for selecting cloud service providers called *Consensus Cloud Assessment Initiative* (CAI), a questionnaire that allows assessing the security management of a provider according to answers. However, this process can be tedious and complex for customers.

Thus, the idea of this project arises: to create a tool that automatically makes that cloud service assessment easily for the customer. This tool would be composed of two parts:

- An engine that manages and analyses data security metrics of cloud services providers and a Web service to access that data.

- A web application that allows to compare graphically the security services from different CSPs using the data provided by the Web service.

The final tool is integrated by two related projects that implement each of the parts as is shown in Figure 1.

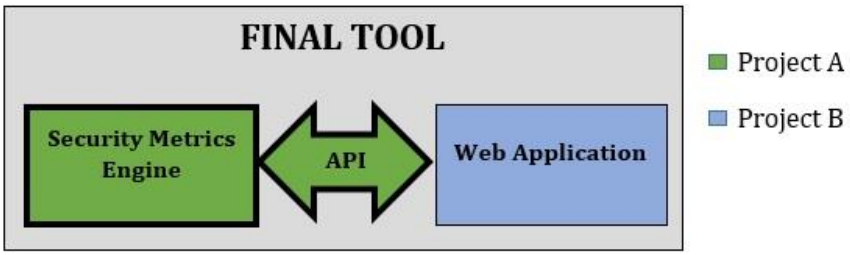

Figure 1. Tool structure

In particular, this project corresponds to the Project A shown in Figure 1. The goal of this project is the analysis of the assessment tools (CAI), provided by the CSA, and developing a processor which gets a new data format based on security metrics and creating a Web service with an API for access to such metadata by other applications.

Finally, both project come together in a joint project to integrate the final tool.

1.2 Objectives

As stated in the previous section, the purpose of this project is to develop a system that manages security metrics associated with cloud service providers by allowing the access via a Web service. For that, it is necessary to satisfy the following specific aims:

- To study security mechanisms of cloud service providers (CSPs). An analysis of the security controls and CAI Questionnaire documents will be performed. Also, providers will be selected based on their metadata structure.

- To elaborate ontology that establishes a common structure for metadata. Therefore, the CAIQ documents structure according to the available versions will be analysed.

- To develop a program to parse the information contained in CAI Questionnaires into the ontology format and to associate metrics to these metadata.

- To install a documental database system to store the metadata.

- To implement a Web service with well-defined an API (Application Programming Interface), which allows the access these metadata by other applications.

- To perform validation and integration tests with the Web application developed in the project B.

1.3 Development phases

In the development of this project the following phases are defined:

- **Technology analysis**: this phase includes the initial planning and the analysis of all technologies and standards that will be used in this project. In this first phase are specially analysed the cloud security documents (CAIQ) of providers included in STAR registry from CSA [12].

- **Design of solution**: this phase comprises the processes about definition of developed system and its components, functional and non-functional requirements, alternative solutions, ontology elaboration and cloud service providers selection.

- **System implementation**: the third phase defines the development of the program that parses metadata to ontology format, installation of database system, which stores the information, and the Web service implementation.

- **Test results**: this phase presents the results of use cases testing, which satisfy the requirements, and integration testing performed by the Web application of Project B.

- **Documentation**: this phase represents the elaboration of this document.

1.4 Document structure

The document is divided into seven chapters:

Chapter 1. Introduction: this chapter presents an overview of the project and indicates the problem description and project aims.

Chapter 2. State of the Art: this chapter analysed standards and technologies used in this project.

Chapter 3. Regulatory Framework: in this point the legal implications of this project are analysed.

Chapter 4. Analysis and Design: this chapter includes a detailed description of the developed system, requirements and the design of possible solutions.

Chapter 5. Implementation and Testing: this point contains the implementation of the designed system in the previous chapter and the tests carried out in order to check its operation.

Chapter 6. Project Management and Costs Estimation: this chapter describes the project development phases and resource estimation.

Chapter 7. Conclusions: finally, the last chapter presents the conclusions and future works of this project.

Annexes: this section presents several annexes of this document, including an example of CAI Questionnaire from one CSP.

2 Estado del Arte

2.1 Ontología

El término **ontología** se refiere a un esquema conceptual o sistema de representación formal definido por una serie de conceptos y relaciones existentes entre ellos, dentro de un dominio o ámbito del conocimiento. Mediante dichas relaciones entre conceptos, restringidos por axiomas, una ontología permite la representación del conocimiento sobre un área determinada [1].

Una ontología determina un esquema o estructura común de comunicación que facilita el intercambio de información entre diferentes entidades o sistemas, garantizando la interoperabilidad entre componentes.

Una de las principales aplicaciones de las ontologías tiene relación con el desarrollo de la web semántica. De esta manera, mediante el uso de ontologías comunes, se integran metadatos semánticos que describan relaciones entre los datos de la red para que sean procesados y evaluados por agentes inteligentes. Esto permitirá realizar búsqueda de datos relacionados entre sí, y no sólo de un modo sintáctico, como ocurre en la web actual.

Otros usos o aplicaciones de las ontologías son: la construcción automatizada de mapas conceptuales, sistemas de bases de conocimiento y lenguajes de representación del conocimiento, así como la extracción de la estructura de los metadatos de documentos para facilitar un formato de intercambio de datos, uso principal de la ontología en este proyecto

2.1.1 Características

Las principales características que presentan las ontologías son las siguientes:

- **Múltiples ontologías**: para la creación de una ontología de carácter general es posible la combinación de varias ontologías que introduzcan conceptualizaciones más específicas. Para ello, debe ser posible relacionar los conceptos de dichas ontologías para establecer generalizaciones, especializaciones y conexiones [2].

- **Niveles de abstracción**: un esquema ontológico contiene varios niveles de conceptos o clases según su grado de abstracción o generalización. Cada nivel otorga mayor especificación [2].

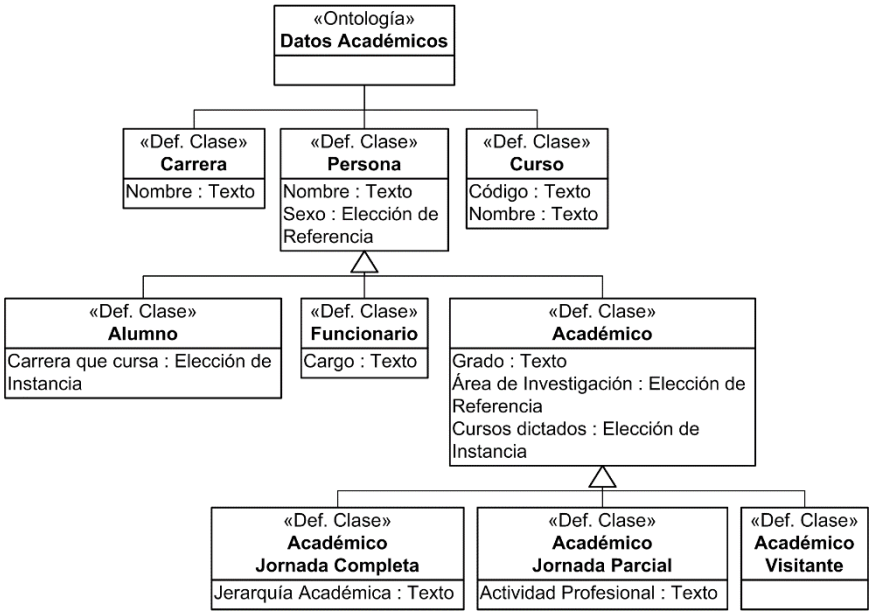

Figura 2. Ejemplo de ontología con distintos niveles de abstracción [3].

- **Multiplicidad de representación**: es posible la existencia de múltiples formas para representar un mismo concepto [2].

Al margen de las características, las ontologías poseen un conjunto de propiedades que deben cumplir [2]:

- **Claridad**: debe comunicar el significado de sus términos de manera efectiva y objetiva.

- **Coherencia**: debe ser posible realizar inferencias consistentes con las definiciones de los conceptos**.**

- **Extensibilidad**: debe permitir extensiones y especializaciones para futuros usos y aplicaciones de la ontología.

- **Precisión**: debe haber el mínimo número de asunciones o suposiciones acerca del dominio o ámbito modelado**.**

2.1.2 Elementos

Como ya se ha introducido, una ontología está compuesta por varios elementos básicos: clases, relaciones, funciones, axiomas e instancias.

Un **concepto** o **clase** es la idea básica de un término, la abstracción de los objetos del dominio. Puede ser un objeto, acción o un método [1]. Las clases pueden contener atributos que describan alguna característica del concepto. Se disponen mediante una estructura jerárquica según los niveles de abstracción, siendo los conceptos superiores más generales.

Las **relaciones** representan la interacción entre las clases dentro del dominio. Sirven de enlace para la creación del mapa conceptual y definen la taxonomía del dominio. Ejemplos de relaciones: es-un, es-subclase-de, conectado-a. Las **funciones** son un tipo especial de relación que contienen las clases además de los atributos.

Los **axiomas** son los teoremas o restricciones que se aplican a las relaciones entre clase y que deben cumplir todos los elementos de la ontología [1].

Por último, las **instancias** son representaciones específicas de objetos de una clase.

2.1.3 Lenguajes

Existen numerosos estándares o lenguajes para la representación de ontologías, entre los que destacan RDF y OWL.

En primer lugar se encuentra **RDF** (*Resource Description Framework*), un lenguaje diseñado por la World Wide Web Consortium (W3C) para la especificación de metadatos. Basado en XML (*eXtensible Markup Language*) es utilizado para el modelado de datos de los recursos implementados en la web mediante la descripción de éstos y las relaciones entre ellos, de manera que pueda ser procesado por las máquinas [4].

A diferencia de otros lenguajes descriptivos como XML, RDF aporta semántica al modelado de datos. RDF permite describir recursos, identificados a través de sus URIs, usando una serie de propiedades y proposiciones simples o declaraciones. Las declaraciones son propiedades con un valor asignado para un recurso específico y se denominan tripletas, una estructura de entidad-atributo-valor.

Posteriormente, la W3C definió un nuevo lenguaje denominado **OWL** (*Web Ontology Language*). Diseñado para ser empleado en aplicaciones o programas que necesitan procesar información contenida en documentos, presentados inicialmente para los humanos, permite publicar y compartir ontologías en la web [5].

Se trata de un lenguaje basado en XML y RDF, por lo que utiliza las tripletas de RDF proporcionando un vocabulario adicional para expresar un mayor significado y semántica de los términos, lo que se traduce en un poder expresivo mayor que su predecesor. Esta característica permite la representación de ontologías explícitamente mediante la definición del significado de los términos, propiedades y relaciones entre clases.

OWL es el estándar actual para el uso de ontologías y el más usado puesto que está construido sobre RDF. OWL contiene tres sub-lenguajes, según el nivel de expresividad que otorgan:

- **OWL Lite**: orientado a aplicaciones que principalmente requieren ontologías con una clasificación jerárquica de clases y restricciones simples [5].

- **OWL DL**: proporciona la máxima expresividad manteniendo garantías de computación (todas las conclusiones computables) y resolución (computaciones resueltas en tiempo finito). Incluye todas las funcionalidades de OWL bajo ciertas restricciones [5].

- **OWL Full**: proporciona máxima expresividad y libertad sintáctica aunque, a diferencia de OWL DL, no otorga garantías computacionales. Este tipo posee mayor flexibilidad y dinamismo aunque no es completamente soportado por cualquier software racional [5].

2.2 Cloud Security Alliance (CSA)

Cloud Security Alliance (CSA) es una organización sin ánimo de lucro dedicada a promover la investigación sobre las mejores prácticas para ofrecer garantías de seguridad en ***Cloud Computing***. Proporciona educación y orientación a las empresas que implementan servicios de *Cloud Computing* [6].

El término *Cloud Computing* se encuentra definido, según el NIST (*National Institute of Standards and Technology*), como “un modelo para habilitar acceso

conveniente bajo demanda a un conjunto compartido de recursos computacionales, por ejemplo, redes, servidores, almacenamiento, aplicaciones y servicios, que pueden ser rápidamente aprovisionados y liberados con un esfuerzo mínimo de administración con el proveedor de servicios" [7].

La organización fue creada en 2008 con el fin de orientar a empresas y compañías en el uso de la nube. Actualmente cuenta con más de 400 voluntarios trabajando en diferentes investigaciones.

La compañía trabaja en varias áreas de investigación que incluyen artículos, estándares y herramientas. Algunas de dichos grupos de trabajo son las siguientes:

- GRC (*Governance, Risk and Compliance*) *Stack* [8].
- STAR (*Security, Trust & Assurance Registry*) [8].
- *Top Threats*: el objetivo de este grupo de trabajo es asesorar sobre los riesgos y amenazas presentes en las diferentes estrategias de adopción de la nube [8].
- *Software Defined Perimeter (SDP)*: iniciativa cuyo objetivo es proteger la infraestructura de las aplicaciones de los ataques basados en la red [8].
- SecaaS (*Security as a Service)*: investigación dedicada al desarrollo del modelo de servicio Cloud centrado en la seguridad de la nube [8].

El grupo de trabajo GRC *Stack* trata de una serie de herramientas proporcionadas por la CSA a las empresas para evaluar sus servicios Cloud de acuerdo con los estándares y requisitos de cumplimiento. Puede dividirse en cuatro secciones: *Cloud Audit*, CCM, CAI y CTP (*Cloud Trust Protocol*) [8].

A continuación se trata las secciones de **CCM**, **CAI** y **STAR**, temas clave en el desarrollo del proyecto.

2.2.1 *Cloud Control Matrix* (CCM)

CCM es un proyecto desarrollado por la CSA que consiste en una matriz de controles de referencia que incorpora las especificaciones para la seguridad de los servicios Cloud. El objetivo es proporcionar a los proveedores de servicios de Cloud Computing una lista con los principales controles de seguridad que sus servicios requieren. Por otro lado, es de utilidad para los clientes de dichos

proveedores para evaluar la seguridad y los riesgos en la adopción de los servicios Cloud.

En la matriz de controles se recogen un conjunto de controles agrupados en 16 dominios propuestos por la CSA en la versión más reciente del CCM (v3.0.1), como se indica en la Tabla 1:

Dominios	Siglas	Controles
Seguridad de las aplicaciones e interfaces.	AIS	4
Cumplimiento y aseguramiento de las Auditorías	AAC	3
Gestión de la continuidad del negocio y resiliencia operacional	BCR	11
Control de cambios y gestión de la configuración	CCC	5
Seguridad de datos y gestión del ciclo de vida de la información	DSI	7
Seguridad del centro de datos	DCS	9
Gestión de caves y cifrado	EKM	4
Gobierno y gestión del riesgo	GRM	11
Recursos humanos	HRS	11
Gestión de identidades y accesos	IAM	13
Seguridad de la infraestructura y virtualización	IVS	13
Interoperabilidad y portabilidad	IPY	5
Seguridad móvil	MOS	20
Gestión de incidentes de seguridad, localización de evidencias electrónicas, investigaciones forenses en la nube	SEF	5
Gestión de cadena de suministro, transparencia y responsabilidad	STA	9
Gestión de vulnerabilidades y amenazas	TVM	3

Tabla 1. Lista de los dominios, siglas y número de controles por dominio de CCM v3.0.1.

En el documento se encuentran todos los controles detallados para favorecer su comprensión por parte de proveedores y clientes. El documento muestra la relevancia del control en distintas arquitecturas (físicas, de red, de cómputo, almacenamiento, aplicación y datos). También se indica el modelo de servicio Cloud que aplica, siendo SaaS, PaaS o IaaS, así como la importancia que posee para el gobierno de la corporación.

Otro aspecto útil que posee el documento es la correspondencia de los controles de la CSA con los diferentes estándares de la industria, entre ellos: ISACA COBIT, ISO/IEC 27001-2005, PCI-DSS y NIST SP800-53 R3. De esta manera, los

proveedores aseguran la consistencia de las decisiones de seguridad de acuerdo con las normas y estándares de los diferentes ámbitos de la industria [9].

2.2.2 *Consensus Assessment Initiative* (CAI)

Consiste en una iniciativa orientada a proporcionar transparencia en los servicios Cloud mediante la documentación de los controles de seguridad de dichos servicios. El resultado es la creación de un documento denominado **CAIQ** (*CAI Questionnaire*).

Basado en el sistema de controles del CCM, presenta una serie de preguntas para los distintos controles que el proveedor o el cliente contesta con el fin de evaluar la seguridad del servicio. Además, al igual que en el caso del CCM, existe una correspondencia entre los controles de CSA con los demás estándares regulatorios.

A continuación en la Figura 3 se ilustra la estructura que sigue el cuestionario para un ejemplo de control:

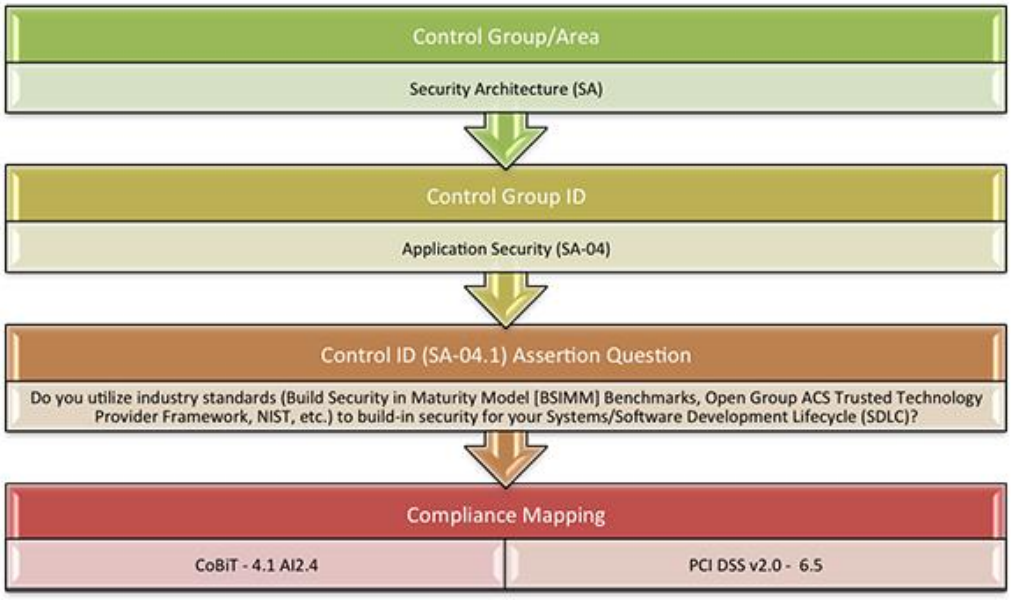

Figura 3. Funcionamiento del CAI Questionnaire para un control específico [9].

CAIQ y CCM se complementan debido al hecho de que ambos están basados en el mismo sistema de controles. De esta manera, las organizaciones utilizan ambos para obtener una lista detallada de los controles y requisitos que desean que sus proveedores de servicios Cloud implementen.

Las métricas y datos utilizados en el proyecto para su gestión provienen de los documentos CAI Questionnaire de los proveedores. En capítulos siguientes se detalla el proceso del tratamiento de estos datos para su posterior manipulación.

2.2.3 Registro de Seguridad, Confianza y Garantías (STAR)

STAR es un mecanismo de certificación de proveedores Cloud a través de un registro público que contiene los controles de seguridad proporcionados por los proveedores (CCM y CAIQ), además del nivel de certificación del proveedor. Se trata de una iniciativa conjunta de CSA y *British Standard Institution* (BSI). STAR de basa en *Open Certification Framework* (OCF), un entorno de control que ofrece a los proveedores un esquema de certificación de confianza global [11].

El entorno OCF se dispone en tres niveles, según el nivel de validación y certificación [12]:

- **Nivel 1:** consiste en una autoevaluación del grado de cumplimiento de los controles del CCM por parte del proveedor. Para ello, dicho proveedor responde a las preguntas del cuestionario CAIQ y se publica en el registro. Es el nivel más bajo de certificación.

- **Nivel 2:** el segundo nivel se divide en varios sub-niveles.

    - **Garantía STAR:** en este sub-nivel un auditor independiente garantiza el nivel de control del proveedor mediante el CCM y los criterios del estándar SOC 2 (*Service Organization Controls report*).

    - **Certificación STAR:** consiste en una auditoría independiente a través de una tercera parte que valida el cumplimiento de los controles por parte del proveedor, utilizando los requisitos de la norma ISO/IEC 27001:2005, así como el CCM. Las auditorías independientes sólo son realizadas por organismos de certificación cualificados, como la anteriormente mencionada BSI.

    - **Evaluación C-STAR:** se trata de una evaluación independiente de terceros dirigida al mercado de la Gran China con el fin de alinear los controles de CSA con las normas nacionales chinas. C-STAR utiliza los requisitos de la norma GB/T 22080-2008 y el CCM para la evaluación.

- **Nivel 3:** este nivel consiste en una certificación basada en monitorización continua. De esta manera, el proveedor proporciona información en tiempo real para conseguir una validación continua [10].

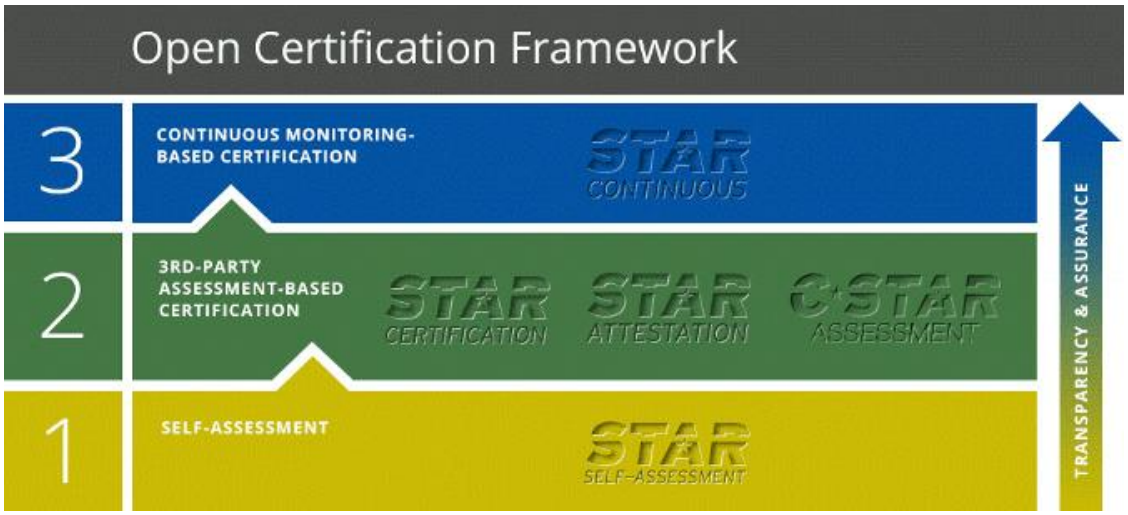

Figura 4. Niveles de certificación del entorno OCP del CSA-STAR [12].

A partir del registro STAR se obtienen los documentos CAIQ de los cuales se extraen los metadatos de seguridad.

2.3 Servicios Web

Los servicios web pueden definirse como un conjunto de tecnologías con capacidad para interoperabilidad entre máquinas en la web, mediante el uso de estándares y protocolos para el intercambio de datos entre aplicaciones [13].

Las organizaciones responsables de la estandarización y arquitectura de los servicios web son la W3C y OASIS (*Organization for the Advancement os Structured Information Standards*). Su misión es la integración de estándares que garanticen la interoperabilidad de los servicios web.

Existen diferentes arquitecturas de los mecanismos de comunicación entre las aplicaciones. El caso más común se refiere a los servicios web basados en **SOAP** (*Simple Object Access Protocol*), que consiste en la comunicación entre servidores y clientes mediante mensajes XML.

SOAP es un protocolo estándar que permite la interacción entre procesos mediante el intercambio de datos XML. Los datos pueden ser enviados mediante HTTP o SMTP, entre otros. Los datos XML se encapsulan en un mensaje SOAP, formados por una cabecera y un cuerpo. Para que un cliente acceda a un servicio, SOAP necesita de una capa adicional, WSDL (*Web Service Description Language*). WSDL permite establecer un acuerdo o contrato entre servidor y cliente, especificando los detalles del mecanismo de transporte de mensajes y sus sintaxis [14].

Sin embargo, en los últimos años ha surgido un nuevo estilo de arquitectura software denominado **REST** (*REpresentational State Transfer*), que ha dado lugar a servicios web basados en REST o servicios RESTful.

2.3.1 Servicios RESTful

REST es un estilo de arquitectura software para sistemas hipermedia distribuidos, como la web, basado en el uso del protocolo **HTTP**. El término REST fue acuñado por primera vez por Roy Fielding en su tesis doctoral en el año 2000, uno de los autores del protocolo HTTP [14].

REST permite crear servicios que permitan la transmisión de información a través de estándares como HTTP y XML sin necesidad de utilizar una capa adicional que especifique los detalles del intercambio de mensajes, como es el caso de SOAP y WSDL. De esta manera es posible crear APIs accesibles por cualquier cliente de manera más simple que con los servicios web anteriores.

A diferencia de SOAP, el cliente no accede a servicios sino a recursos. Dichos recursos pueden estar representados no sólo en formato XML, también en forma de texto o en formato **JSON**, que proporciona mayor simplicidad en la representación de datos.

Para que un servicio REST o RESTful sea considerado como tal debe poseer las siguientes características:

- **Sistema cliente-servidor**: es una arquitectura donde existe una separación clara entre cliente y servidor, siendo ambos independientes. Los clientes acceden directamente a los recursos independientemente de las operaciones que se lleven a cabo en el servidor. Esta separación de las responsabilidades proporciona una alta flexibilidad a los servicios REST [16].
- **Sin estado**: en los servicios RESTful, servidor y cliente no mantienen el estado de la comunicación debido a que HTTP es un protocolo sin estado. Por tanto, toda petición HTTP debe contener la información necesaria para comprender la consulta. Sin embargo, esta característica resta seguridad a este tipo de servicios, aunque, en la práctica, se utilizan cookies y demás mecanismos para mantener la sesión del cliente [16].

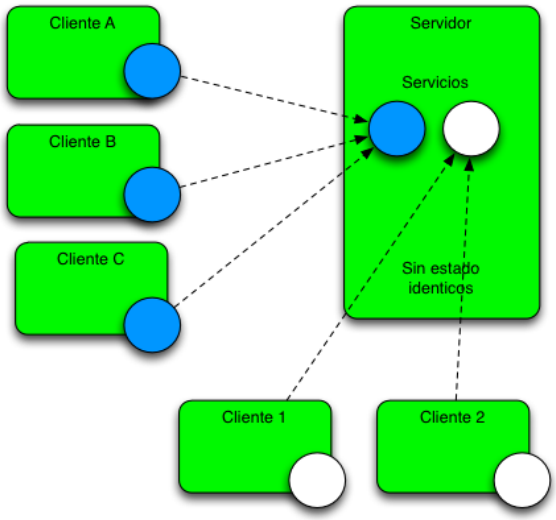

Figura 5. Esquema peticiones sin estado en servicio RESTful [16].

- **Caché**: el contenido de los recursos puede almacenarse en caché de manera que en peticiones posteriores se pueda acceder a esos datos si fuera necesario. Esta característica aumenta la escalabilidad puesto que un cliente REST no distingue si la petición se realiza directamente al servidor o a un sistema de cachés [16].

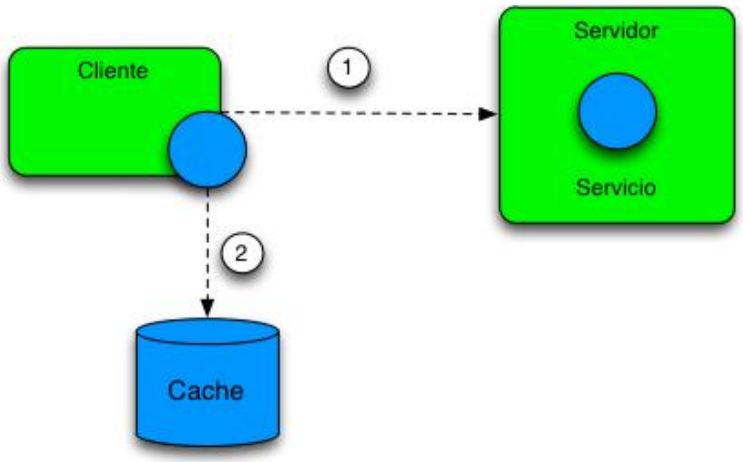

Figura 6. Esquema sistema caché REST [15].

- **Accesibilidad**: el acceso a los recursos se realiza a través de identificadores globales, las URIs (*Universal Resource Identifier*). De esta manera, se identifica de forma única al recurso en el API. La URI tiene una estructura definida:

```
{protocolo}://{dominio o hostname}[:puerto]/{ruta del
recurso}?{consulta de filtrado}
```

- **Servicios uniformes y operaciones**: los servicios REST deben tener un conjunto de operaciones definidos y comparten un mecanismo de invocación de los recursos uniforme. Esto se lleva cabo utilizando las principales operaciones que ofrece HTTP: GET, POST, PUT y DELETE. El método GET obtiene la representación de un recurso. Los métodos POST y PUT añaden o modifican un recurso. Por último, con DELETE se elimina un recurso [14].

- **Representación de los recursos**: REST soporta múltiple tipos de representación de los datos. A diferencia de SOAP, que sólo utiliza XML, los servicios REST también permite texto y formato JSON, entre otros. Este último es especialmente utilizado como alternativa a XML debido a su simplicidad, como se detalla a continuación [15].

2.3.2 JSON

JSON (*JavaScript Object Notation*) es un formato ligero para el intercambio de datos. Basado en el estándar ECMA-262, un subconjunto del lenguaje de programación JavaScript, proporciona una alternativa al lenguaje de marcado XML respecto a la representación e intercambio de datos [17].

En la actualidad, el uso del formato JSON en las aplicaciones web ha aumentado en detrimento de XML debido a su mayor simplicidad y legibilidad, tanto para el humano como para la máquina. La simplicidad de JSON es una característica muy útil al trabajar con grandes volúmenes de datos, siendo más cómodo y manejable que XML. Además, se trata de un formato de texto compatible con la gran mayoría de los lenguajes de programación (C, C++, Java, Python y JavaScript, entre otros), por lo que es habitual su uso en el desarrollo de servicios web.

JSON se constituye de dos estructuras soportadas por cualquier lenguaje de programación [17]:

- Una colección de pares nombre/valor, conocido en los lenguajes como *objeto.* El objeto comienza una apertura de llave ({) y concluye con una llave de cierre (}). Comprendido entre las llaves se encuentra el conjunto desordenado de pares nombre/valor separados por una coma (,). En cada par, nombre y valor se encuentran separados por dos puntos (:).

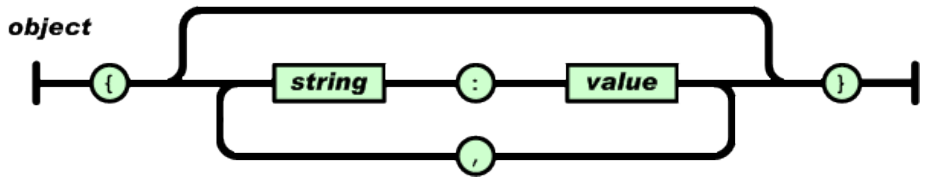

Figura 7. Estructura objeto JSON [17].

- Una colección ordenada de valores, correspondiente a los *arrays*. La estructura de los arrays coincide con los demás lenguajes, una lista de valores ordenados separador por comas (,) comprendidos entre dos corchetes ([ ]).

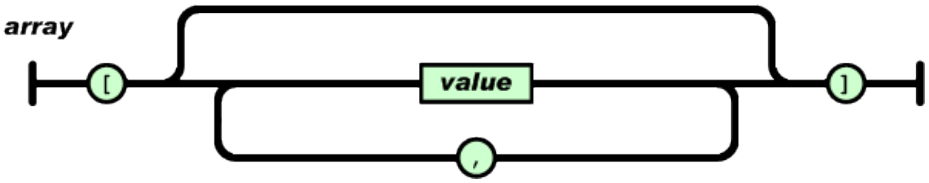

Figura 8. Estructura array JSON [17].

El campo del nombre es una cadena de caracteres o String, comprendido entre dobles comillas. El valor puede ser un número, cadena, booleano o, a su vez, un objeto o array JSON.

El intercambio de datos en los servicios web no es la única finalidad de este formato. También es utilizado en el almacenamiento de información en bases de datos no relacionales, como MongoDB.

2.4 Tecnologías utilizadas

A continuación se encuentran detalladas las diferentes tecnologías y herramientas utilizadas en el desarrollo del proyecto:

2.4.1 Protégé

Protégé es una herramienta de software libre creada por la Universidad de Stanford para la elaboración de ontologías y modelos de representación del conocimiento. El programa se encuentra escrito en Java, permitiendo la compatibilidad con numerosas aplicaciones. Las ontologías creadas pueden ser exportadas en varios formatos como RDF, RDF Schema, XML Schema y, principalmente, OWL [18].

Esta herramienta no precisa instalación, lo cual proporciona flexibilidad en el desarrollo de proyectos. También existe una versión web del programa, WebProtégé, que supone mayores facilidades de uso. Además, contiene una serie de extensiones o *plugins* que pueden ser descargados para añadir funcionalidades, como la visualización de grafos ontológicos o herramientas de evaluación y comprobación de ontologías.

2.4.2 Apache Tomcat

Tomcat es un contenedor de *servlets* desarrollado por Apache Software Foundation que implementa las especificaciones de Java Servlets y JavaServer Pages (JSPs). Como contenedor de *servlets*, su función consiste en recibir peticiones HTTP y redireccionarlas a un *servlet*. El contenedor Tomcat funciona sobre un servidor HTTP Apache y la máquina virtual de Java.

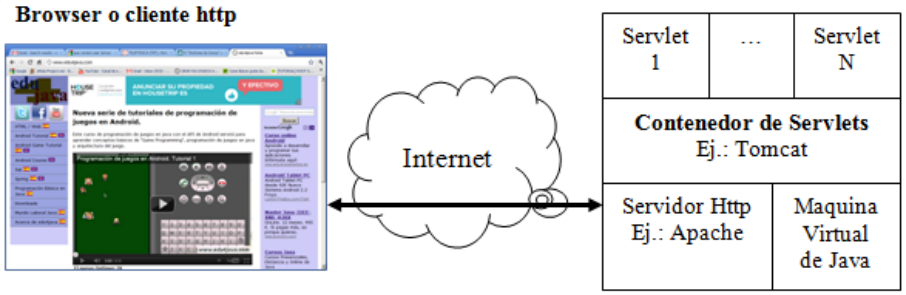

Figura 9. Esquema del funcionamiento de Apache Tomcat [19].

Se trata de una herramienta de software libre desarrollada en Java, siendo una de las más utilizadas como servidor web para aplicaciones debido a su compatibilidad con cualquier sistema operativo que posea la máquina virtual Java. Las primeras versiones fueron las 3.0.x, hasta llegar a las versiones actuales 8.x. En este proyecto en concreto se utiliza la versión 8.0.24, última versión estable de Tomcat.

La estructura de los directorios principales de Tomcat se dispone de la siguiente manera [20]:

- /bin: incluye el arranque y cierre del servidor y otros ejecutables.
- /conf: contiene los ficheros XML y los correspondientes DTD (*Document Type Definition*) para la configuración de Tomcat.
- /logs: almacena los logs de Catalina y las aplicaciones.
- /webapps: contiene las aplicaciones web desarrolladas.

2.4.3 *Framework* JAX-RS (Jersey)

Java API for RESTful Web Services (JAX-RS) es una herramienta que permite el desarrollo de manera sencilla de servicios web de tipo RESTful. JAX-RS, definido en JSR-311, tiene como implementación de referencia de calidad el framework Jersey. Jersey proporciona un soporte para implementar servicios web REST con Java y su máquina virtual [21].

Jersey contiene librerías que permiten desarrollar la API REST como un servicio web en un contenedor de *servlets*, en este caso, Tomcat. Este framework proporciona una serie de anotaciones que simplifican el despliegue de los servicios web y el tratamiento de las peticiones HTTP. Las anotaciones permiten establecer las propiedades de los métodos que atienden las peticiones. Dentro de ese conjunto de anotaciones destacan:

- @Path: especifica la ruta relativa de acceso al recurso REST o método que demanda la petición.

- @GET, @POST: indican que el método responde a una petición HTTP de tipo GET o POST.

- @Produces: define el tipo MIME que presenta la respuesta a la petición. El tipo puede ser: texto plano, texto HTML, XML o JSON, entre otros.

- @Consumes: define los tipos aceptados para los parámetros de la consulta HTTP.

2.4.4 MongoDB

Es un sistema de bases de datos **NoSQL** de código abierto, desarrollado en C++. Se trata de una base de datos orientada a documentos. A diferencia de las bases de datos relacionales, donde los datos se disponen en tablas, en MongoDB se almacenan en documentos de tipo JSON (BSON, representación binaria de JSON) [22].

Una característica importante de las bases datos MongoDB es la replicación maestro-esclavo. La replicación permite implementar varias instancias de la base de datos para asegurar la disponibilidad de los datos y reducir los riesgos de pérdida. La instancia maestra realiza operaciones de escritura y lectura, mientras que las esclavas sólo pueden encargarse de las lecturas. Esta característica, unida a la fragmentación o *sharding*, otorgan escalabilidad al sistema.

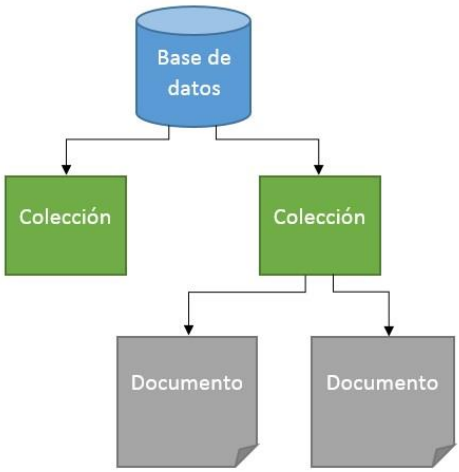

Figura 10. Estructura de datos en MongoDB.

Los datos JSON almacenados se denominan documentos y éstos se guardan en colecciones. Las colecciones se corresponderían con las tablas en una base de datos SQL, y los documentos con los registros de las tablas. Sin embargo, la gran diferencia de los registros de las tablas, no es necesario un esquema común para los documentos de una colección. Cada documento posee su propia estructura mediante un sistema de pares clave-valor, al igual que JSON.

Las consultas a una base de datos MongoDB se puede realizar mediante un programa utilizando las librerías correspondientes, o a través de una consola incluida en MongoDB. En la consola, las consultas se realizan utilizando el lenguaje JavaScript, lo que facilita las consultas a la base por un servicio web, aunque existen extensiones para realizar consultas en otros lenguajes como Java, C, C++ o PHP [23].

Entre las múltiples aplicaciones de MongoDB destaca su uso en entornos que requieran escalabilidad, como almacenamiento de páginas web o sistemas de manejo de documentos.

2.4.5 API

El término API (*Application Programming Interface*) se refiere al conjunto de funciones, subrutinas y herramientas que permite la interacción entre

componentes software. Dicha comunicación entre módulos de software independientes consigue capacidad de abstracción en la programación [24].

Existen varios tipos de implementaciones de APIs según su aplicación. Por un lado, se utiliza en programación como bibliotecas que incluyen una serie de funciones o métodos que pueden ser invocados para implementar una determinada funcionalidad. Un ejemplo de este tipo son las librerías disponibles en los distintos lenguajes de programación para el desarrollo de programas y aplicaciones.

Por otro lado, el uso de APIs también es clave en los servicios web. Mediante la interfaz es posible la interacción y el intercambio de datos entre aplicaciones haciendo uso de llamadas a métodos remotos con peticiones HTTP, como ocurre en los servicios REST.

2.4.6 Office Open XML

Office Open XML es un estándar abierto para documentos de procesamientos de texto, presentaciones y hojas de cálculo que muchas aplicaciones pueden implementar libremente en varias plataformas. Office Open XML está diseñado para representar dichos documentos que están codificados en formatos binarios que definen las aplicaciones de Microsoft Office [25].

El estándar Office Open XML fue creado para permitir la manipulación de los documentos por otras aplicaciones sin importar el formato interno. Estos archivos se encapsulan en un archivo ZIP y contiene una jerarquía de directorios con elementos XML y relaciones que componen la estructura interna del documento. Cada elemento .xml representa un tipo de contenido del documento (diapositivas, hojas de cálculo o gráficas). Los elementos .rels contienen relaciones explícitas para un elemento origen.

Para los documentos Excel (libros de hojas de cálculo) se utiliza el marcado **SpreadsheetML**. La estructura de un documento SpreadsheetML contiene un elemento *workbook.xml* que representa el libro de hojas de cálculo y en él se hace referencia a las diferentes hojas. Cada hoja de cálculo de está definida por un fichero *worksheet.xml* independiente. También se incluyen otros elementos como cadenas compartidas, estilos o gráficas (Figura 11).

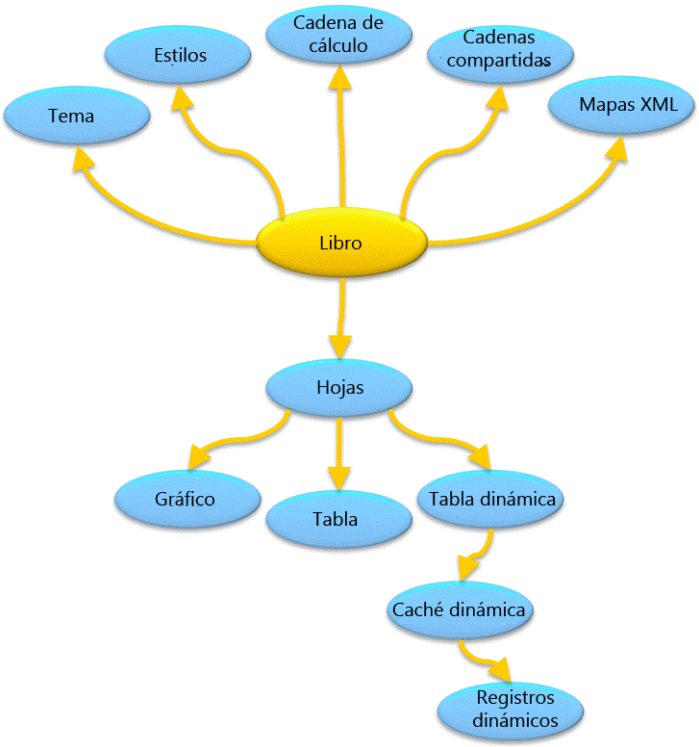

Figura 11. Estructura básica hoja de cálculo SpreadsheetML [25].

3 Marco regulador

En este apartado se analizan las implicaciones legales que afectan al desarrollo del proyecto. En el sistema desarrollado no se hace uso de datos personales que supongan implicaciones relativas a la Ley Orgánica de Protección de Datos. Sólo es necesario el análisis las licencias de las herramientas software utilizadas.

El servidor web utilizado en el proyecto se implementa usando Apache Tomcat, que se encuentra bajo la licencia ***Apache Software License 2.0***. *Apache Software License* 2.0 (ASL 2.0) se trata de una licencia de software libre creada por la *Apache Software* Foundation (ASF) para dar soporte al desarrollo de proyectos. Se trata de una licencia permisiva que proporciona al usuario libertad de modificación, reproducción o distribución. No incluye una cláusula copyleft, por lo que no exige la redistribución de las obras derivadas del proyecto bajo la misma licencia [26].

El uso de la base de datos MongoDB se encuentra bajo la licencia **GNU AGPL v3.0**, una licencia copyleft de software libre. Pese a ser una licencia copyleft, el simple uso de MongoDB en las aplicaciones no está afectado por dicha cláusula. Sólo en el caso de modificación del código fuente es necesaria la publicación de la nueva versión [27].

La herramienta Protégé utilizada en el proyecto posee una licencia ***Berkeley Software Distribution*** (**BSD**), licencia de código libre que permite el uso totalmente libre del software, incluso comercial [28].

4 Análisis y Diseño

En este capítulo se realizará una descripción detallada del sistema en desarrollo. Se presentarán las funciones y requisitos que debe implementar y cumplir, justificando las decisiones del uso de las diferentes tecnologías frente a las alternativas. Una vez analizado los requerimientos, se presentará la arquitectura del sistema especificando los diferentes módulos que lo componen, así como una descripción del entorno de desarrollo utilizado, el proceso de selección de los proveedores de servicios cloud y las métricas de seguridad utilizadas.

4.1 Definición del sistema

El proyecto consiste en el diseño e implementación de un sistema que permita extraer información, contenida en los documentos CAIQ en formato Excel (.xlsx), relativa a las métricas de seguridad de los servicios Cloud de una serie de proveedores y la exposición de una API para el acceso a dichos metadatos a través de la web. A continuación se realiza el análisis de los requisitos del sistema diseñado.

4.1.1 Requisitos

Existen dos tipos de requisitos: funcionales y no funcionales. Por un lado, los requisitos **funcionales** definen el comportamiento del sistema en cuanto a las funcionalidades que debe implementar. Por otro lado, los requisitos **no funcionales** se centran en la implementación de las funcionalidades del sistema, imponiendo restricciones sobre dichas funcionalidades definidas en los requisitos funcionales.

La especificación de los requisitos se realiza mediante una serie de tablas, cuya plantilla se muestra en la Tabla 2:

ID:					
Nombre					
Prioridad		**Necesidad**		**Tipo de requisito**	
Descripción					

Tabla 2. Plantilla de requisitos.

Los campos de la Tabla 2 de requisitos se definen de la siguiente manera:

- ID: identificador del requisito con formato R-[número de requisito].
- Nombre: indica el nombre del requisito.
- Prioridad: indica la prioridad de implementación del requisito, tomando valores Alta, Media o Baja.
- Necesidad: establece el nivel de importancia del requisito en el desarrollo del sistema, según los valores Esencial, Deseable u Opcional.
- Tipo de requisito: indica si se trata de un requisito funcional o no funcional.
- Descripción: incluye una descripción del requisito.

A continuación se muestran los requisitos funcionales y no funcionales siguiendo la plantilla de la tabla de requisitos:

ID: R-01					
Nombre	Procesamiento de documentos CAIQ.				
Prioridad	Alta	**Necesidad**	Obligatorio	**Tipo de requisito**	Funcional
Descripción	El sistema deberá ser capaz de procesar los documentos CAIQ en formato .xlsx (SpreadsheetML).				

Tabla 3. Requisito funcional R-01.

ID: R-02					
Nombre	Cantidad de proveedores.				
Prioridad	Alta	**Necesidad**	Deseable	**Tipo de requisito**	Funcional
Descripción	El sistema deberá ser capaz de procesar información de la mayor cantidad de proveedores posible.				

Tabla 4. Requisito funcional R-02.

ID: R-03					
Nombre	Métricas de seguridad.				
Prioridad	Alta	**Necesidad**	Obligatorio	**Tipo de requisito**	Funcional
Descripción	El sistema deberá ser capaz de asociar métricas de seguridad a los metadatos procesados.				

Tabla 5. Requisito funcional R-03.

ID: R-04					
Nombre	Lista de proveedores.				
Prioridad	Alta	**Necesidad**	Obligatorio	**Tipo de requisito**	Funcional
Descripción	El usuario podrá acceder a la lista de proveedores disponibles.				

Tabla 6. Requisito funcional R-04.

ID: R-05					
Nombre	Lista de criterios de seguridad.				
Prioridad	Alta	**Necesidad**	Obligatorio	**Tipo de requisito**	Funcional
Descripción	El usuario podrá acceder a la lista de criterios de seguridad contenidos en los metadatos, con varios niveles de detalle.				

Tabla 7. Requisito funcional R-05.

ID: R-06					
Nombre	Lista de valores de métricas de seguridad.				
Prioridad	Alta	**Necesidad**	Obligatorio	**Tipo de requisito**	Funcional
Descripción	El usuario podrá acceder a la lista de valores de las métricas asociadas a los criterios de seguridad con varios niveles de detalle, para uno o todos los proveedores.				

Tabla 8. Requisito funcional R-06.

ID: R-07					
Nombre	Información adicional.				
Prioridad	Baja	**Necesidad**	Opcional	**Tipo de requisito**	Funcional
Descripción	El usuario podrá acceder al metadato CAIQ completo para un proveedor concreto como información adicional.				

Tabla 9. Requisito funcional R-07.

ID: R-08					
Nombre	Acceso a recursos.				
Prioridad	Alta	**Necesidad**	Deseable	**Tipo de requisito**	Funcional
Descripción	El usuario podrá acceder a los recursos fácilmente a través de su URI.				

Tabla 10. Requisito funcional R-08.

ID: R-09					
Nombre	Lenguaje de programación.				
Prioridad	Media	**Necesidad**	Deseable	**Tipo de requisito**	No funcional
Descripción	El sistema será desarrollado utilizando el lenguaje de programación Java.				

Tabla 11. Requisito no funcional R-09.

ID: R-10					
Nombre	Base de datos.				
Prioridad	Alta	**Necesidad**	Deseable	**Tipo de requisito**	No funcional
Descripción	El almacenamiento de los metadatos se deberá realizar mediante un sistema de bases de datos acorde con el formato de los metadatos.				

Tabla 12. Requisito no funcional R-10.

ID: R-11					
Nombre	Formato de datos.				
Prioridad	Alta	**Necesidad**	Deseable	**Tipo de requisito**	No funcional
Descripción	Los datos procesados deben ser almacenados en un formato fácilmente manejable por aplicaciones web.				

Tabla 13. Requisito no funcional R-11.

4.1.2 Elección de tecnologías y alternativas

A continuación se plantearán las diferentes soluciones posibles para los requisitos del sistema.

En primer lugar, el formato de los metadatos puede definirse en base a dos alternativas: **XML** o **JSON**. El uso de XML sería válido debido a que los documentos CAIQ son de tipo Excel (SpreadsheetML), cuya estructura interna se encuentra codificada en XML. Sin embargo, se toma como elección la utilización del formato JSON porque proporciona mayor manejabilidad y facilidad para la manipulación de datos, aunque no es la única razón para su elección.

Para el despliegue del **servicio web** que gestione las peticiones a la API, se ha decantado por el uso de una API basada en servicios **REST**, una arquitectura orientada a recursos. Otra alternativa sería utilizar servicios web basados en **SOAP**, mediante datos en formato XML. Sin embargo, resulta más sencillo crear APIs con servicios REST que con SOAP. Además, SOAP sólo soporta XML, mientras que REST también permite el uso de JSON. El almacenamiento de datos JSON en una base documental es más ágil y simple que el formato XML. Ésta es otra razón para el uso de este tipo de formato de datos.

En cuanto a la base de datos, las necesidades del proyecto requieren una base de datos no relacional o documental. Esto se debe a que la información almacenada serán objetos JSON. Por tanto, no tendría sentido el uso de una base de datos SQL basada en tablas.

4.2 Entorno de desarrollo

En este apartado se especifica el entorno de desarrollo software utilizado en la implementación de los distintos bloques del sistema.

4.2.1 Herramientas software

Las herramientas software utilizadas son las siguientes:

- Protégé v5.0.0: herramienta de código abierto para la elaboración y edición de la ontología que define la estructura de los metadatos.

- OntoGraf: *plug-in* de Protégé para la representación gráfica de la estructura de clases y relaciones que componen la ontología.

- IDE Eclipse MARS: entorno de desarrollo utilizado en la programación del bloque procesador de documentos CAIQ y en la aplicación web de la API REST.

- UML Lab v1.8.0: *plug-in* de Eclipse para la visualización de diagramas UML de clases.

- Java Development Kit (JDK) 1.8.0_45: herramienta para el desarrollo de aplicaciones y programas basados en Java.

- MongoDB v3.0.4: base de datos NoSQL utilizada para el almacenamiento de los metadatos del documento CAIQ.

- Apache Tomcat v8.0.24: servidor web de software libre donde se realiza el despliegue de la API.

4.2.2 Lenguaje de programación

El lenguaje utilizado en el proyecto es Java, tanto para el programa procesador de documentos como para la aplicación web que implementa la API. La elección de este lenguaje es debido a su extendido uso y a la existencia de numerosos entornos, herramientas y *frameworks* para el desarrollo de aplicaciones Java.

4.3 Diseño

A continuación se presenta el diseño del sistema descrito en el análisis anterior, cómo se ha estructurado y la descripción de los distintos bloques o módulos.

4.3.1 Arquitectura

El sistema se encuentra dividido en tres bloques diferenciados: el programa procesador de los documentos CAI Questionnaire, la base de datos y el servidor web, como se puede ver en la Figura 12. Todos los módulos son transparentes al usuario que realice las peticiones, únicamente se comunica a través de las llamadas a recursos expuestas en la API.

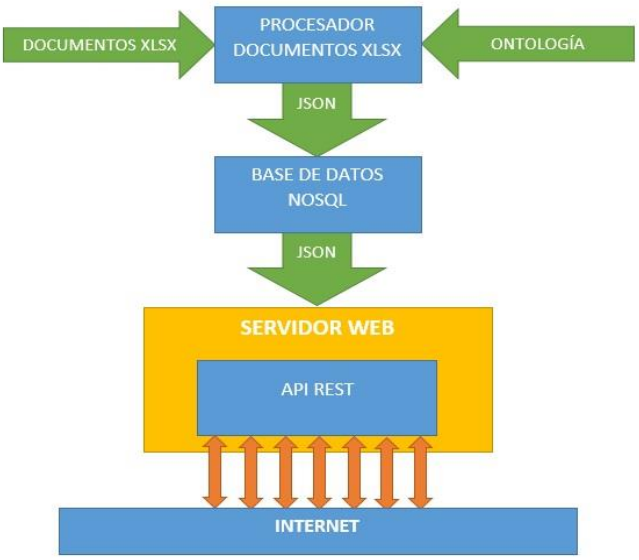

Figura 12. Arquitectura global del sistema.

4.3.2 Documentos CAIQ

Los documentos iniciales utilizados se denominan *Consensus Assessment Initiative Questionnaire* (CAIQ). Se trata de un documento Excel que contiene un cuestionario, en forma de tabla, acerca de los diferentes controles de seguridad que un servicio Cloud determinado cumple. Dichos documentos son proporcionados por los proveedores como evaluación de sus servicios en la nube. Existen, principalmente, dos versiones del documento: versión 1.1 y 3.0.1. La versión 1.1 posee algunos aspectos diferentes a la versión más reciente. Dichas diferencias se explican más adelante.

Control Group	CGID	CID	Control Specification	Consensus Assessment Questions	Consensus Assessment Answers		
					Yes	No	Not Applicable
Datacenter Security *User Access*	DCS-09	DCS-09.1	Physical access to information assets and functions by users and support personnel shall be restricted.	Do you restrict physical access to information assets and functions by users and support personnel?	Yes		
Encryption & Key Management *Entitlement*	EKM-01	EKM-01.1	Keys must have identifiable owners (binding keys to identities) and there shall be key management policies.	Do you have key management policies binding keys to identifiable owners?	Yes		

Tabla 14. Extracto (I) de un ejemplo de CAI Questionnaire v3.0.1.

Como se puede observar en la Tabla 14, ésta contiene varias categorías. La categoría Control Group (**CG**) contiene los diferentes grupos que engloban los controles con características comunes. Estos grupos se engloban en **dominios**, representados en el documento con distintos colores. Los dominios están definidos por las diferentes áreas críticas en seguridad en Cloud Computing.

La siguiente columna se corresponde con los identificadores de cada grupo (**CGID**). En el documento también se incluye la descripción de las características del grupo. A continuación, se encuentran los controles básicos, presentado mediante un identificador (**CID**). Cada control se corresponde con una cuestión que debe contestar el proveedor o el usuario que pretende contratar un servicio. De esta manera, se indica si el servicio aplica o no los controles de seguridad y, así, establecer unas métricas relativas a cada control.

El resto de columnas indican la correspondencia entre cada grupo de controles con otros **estándares** existentes en la industria.

Control Group	CGID	CID	AICPA TSC 2009	AICPA Trust Service Criteria (SOC 2SM Report)	AICPA TSC 2014	BITS Shared Assessments AUP v5.0	BITS Shared Assessments SIG v6.0
Datacenter Security *User Access*	DCS-09	DCS-09.1	A3.6.0	(A3.6.0) Procedures exist to restrict physical access to the defined system including, but not limited to, facilities, backup media, and other system components such as firewalls, routers, and servers.	CC5.5	F.2	F.1.2.3, F.1.2.4, F.1.2.5, F.1.2.6, F.1.2.8, F.1.2. 9, F.1.2.10, F.1.2.11, F.1.2.12,

Tabla 15. Extracto (II) de un ejemplo de CAI Questionnaire v3.0.1.

Los metadatos se estructuran siguiendo las categorías del CAIQ. Para ello, se debe confeccionar una ontología que incluya entidades que se correspondan con dichas categorías (CG, CGID, CID y estándares) y las relaciones propias de esas clases. Una vez creada la ontología se exporta al procesador para establecer la estructura de clases necesaria para el manejo de los metadatos.

4.3.3 Procesador de documentos

El módulo procesador de documentos consiste en un programa Java que realiza una conversión de los datos de los documentos **CAIQ** al formato de la ontología definida. Para ello, se debe importar la ontología e integrarla en el programa.

Los documentos Excel están definidos por el estándar Office Open XML como documentos **SpreadsheetML**, cuya estructura interna está compuesta por un conjunto de archivos XML. Por tanto, se trata de un programa procesador de XML. Utilizando las librerías correspondientes se crean objetos de tipo **JSON** con la

estructura definida en la ontología. En este módulo se introducen las **métricas de seguridad** vinculadas a cada uno de los controles.

Una vez obtenidos los metadatos en formato JSON, el programa los almacena en la base de datos documental **MongoDB**.

4.3.4 Base de datos

Para este módulo se hace uso de MongoDB, un sistema bases de datos documental de software libre. Como ya se ha visto, en MongoDB se pueden crear varias bases de datos independientes. A su vez, cada base de datos puede contener colecciones de datos, y en cada colección se almacenan los objetos BSON (JSON) que se deseen. En la Figura 13 se muestra un ejemplo de documento almacenado en MongoDB:


```
{
    "_id":  {
            "$oid": "55f4817b0afa252be4e52e3b"
            },
    "name": "Zscaler",
    "logo": "https://www.zscaler.com/images/znew-logo.png",
    "version": "3.0.1",
    "cg":   {
            "name": "Application & Interface Security"
            }
}
```


Figura 13. Ejemplo de documento en MongoDB.

En este proyecto sólo es necesario el uso de una base de datos, llamada “TFG”, y una colección, llamada “CAIQs”, para almacenar todos los metadatos en forma de objetos JSON.

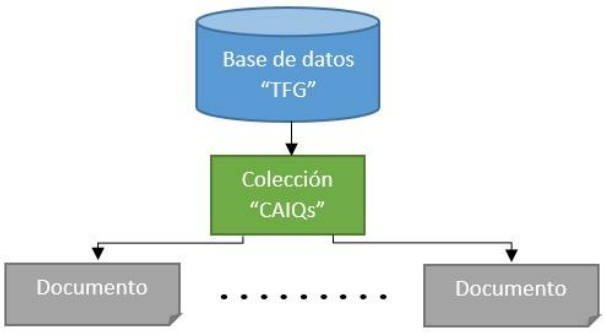

Figura 14. Estructura base de datos MongoDB.

Las consultas a la base de datos son implementadas tanto en el bloque procesador como en el servidor web y se detallan en el capítulo de implementación.

4.3.5 Servidor Web

Este módulo se encuentra dividido en dos partes: el programa que implementa la API y el servidor web sobre el que funciona.

El bloque que implementa la interfaz **API REST** consiste en un programa Java que implementa una serie de métodos correspondientes a las peticiones disponibles. En el programa se obtiene la información requerida para cada petición mediante consultas personalizadas a la base de datos. Se procesan esos documentos (objetos JSON) para retornar el recurso que se demanda en la petición. Los recursos de la API serán accesibles a través de su identificador único URI.

En cuanto al servidor web, consiste en un servidor Apache Tomcat en el cual se integra la aplicación anterior. Tras desplegar el servidor Tomcat, la API se encuentra disponible para realizar peticiones a través de Internet.

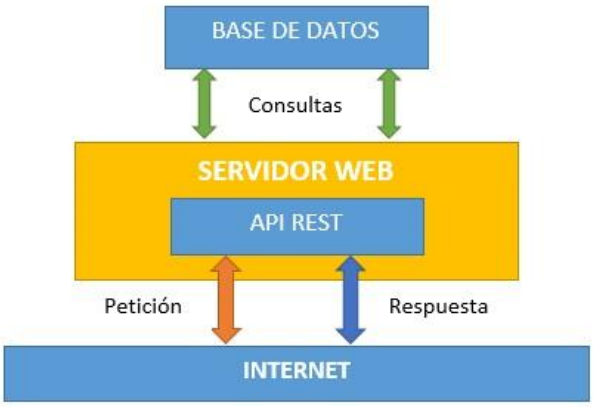

Figura 15. Arquitectura bloque servidor Web.

4.4 Métricas de seguridad

Las métricas introducidas en el módulo procesador consisten en valores numéricos (entre 0 y 1) asignados a los controles de seguridad del documento CAIQ que indican el grado de aplicabilidad de dicho control, y permiten el análisis del servicio en cuestión por otras aplicaciones. En resumen, establecen una medida del nivel de seguridad proporciona un proveedor con sus servicios *Cloud*.

Las métricas son introducidas a nivel de control de seguridad (CID). La asignación de los valores para cada uno de los controles (CID) se realiza en base a las respuestas del proveedor a las preguntas del cuestionario (*Consensus Assessment Questions*) de la siguiente manera:

- Se asigna un valor de 1 al control de seguridad (CID) si la respuesta es Sí (Yes).

- Se asigna un valor de 0 al control de seguridad (CID) si la respuesta es No (No).

- El control de seguridad (CID) es ignorado si la respuesta es No Aplicable (NA).

Las métricas asociadas a la categoría CGID se calculan mediante la agregación de los valores de los controles que engloba dicha categoría. Lo mismo ocurre con las métricas de la categoría CG (dominios), obteniéndose a partir de los valores calculados para cada uno de los CGIDs. El método de cálculo se detalla más adelante en el capítulo de Implementación y Pruebas.

A continuación, en la Tabla 16 se muestra la lista completa de dominios y grupos de controles con su identificador (CGID) sobre los que se aplican las métricas de seguridad. La lista completa de controles (CID), debido a su extensión, se muestra en el ejemplo de CAI Questionnaire (Tabla 23) incluido en el anexo B de la memoria.

Dominios	Grupos de controles	CGID
Seguridad de las Aplicaciones e Interfaces	Seguridad de Aplicaciones	AIS-01
	Requerimientos de Acceso de Clientes	AIS-02
	Integridad de Datos	AIS-03
	Seguridad / Integridad de Datos	AIS-04
Cumplimiento y Aseguramiento de la Auditorías	Planificación de Auditorías	AAC-01
	Auditorías Independientes	AAC-02
	Mapa de Regulación de los Sistemas de Información	AAC-03
Gestión de la Continuidad del Negocio y Resiliencia Operacional	Planificación de la Continuidad de Negocio	BCR-01
	Pruebas de Continuidad de Negocio	BCR-02
	Servicios de infraestructura de los CPD y condiciones medioambientales	BCR-03
	Documentación	BCR-04
	Riesgos medioambientales	BCR-05
	Localización del equipamiento	BCR-06
	Mantenimiento del equipamiento	BCR-07
	Fallos del equipamiento de alimentación	BCR-08
	Análisis de Impacto	BCR-09
	Política	BCR-10
	Política de Retención de Activos	BCR-11
Control de Cambios y Gestión de la Configuración	Compras y Nuevos desarrollos	CCC-01
	Externalización de desarrollos	CCC-02
	Pruebas de Calidad	CCC-03
	Instalaciones no autorizadas de software	CCC-04

	Cambios en producción	CCC-05
Seguridad de los Datos y Gestión del Ciclo de Vida de la Información	Clasificación	DSI-01
	Inventario de Datos / Flujos	DSI-02
	Transacciones de Comercio Electrónico	DSI-03
	Política de seguridad de manejo y etiquetado	DSI-04
	Fugas de Información	DSI-05
	Datos en entornos no de producción	DSI-06
	Propiedad/Servicio de los Datos	DSI-07
Seguridad del Centro de Datos	Gestión de Activos	DCS-01
	Puntos de Acceso Controlados	DCS-02
	Identificación del Equipamiento	DCS-03
	Autorización para extraer activos	DCS-04
	Equipamiento fuera de las instalaciones	DCS-05
	Política	DCS-06
	Autorización de acceso a las Áreas Seguras	DCS-07
	Entrada de Personas	DCS-08
	Acceso de Usuarios	DCS-09
Gestión de Claves y Cifrado	Derechos	EKM-01
	Generación de Claves	EKM-02
	Protección de Datos Sensibles	EKM-03
	Acceso y Almacenamiento	EKM-04
Gobierno y Gestión del Riesgo	Requerimientos básicos	GRM-01
	Enfoque en los datos de las evaluaciones de riesgos	GRM-02
	Supervisión de la Dirección	GRM-03
	Programa de Gestión	GRM-04
	Soporte/Implicación	GRM-05
	Política	GRM-06
	Aplicación de la Política	GRM-07
	Impacto de la Política en las Evaluaciones del Riesgo	GRM-08
	Revisiones de la Política	GRM-09
	Análisis de Riesgo	GRM-10
	Sistema de Gestión del Riesgo	GRM-11
Recursos Humanos	Devolución de Activos	HRS-01
	Comprobación de Antecedentes	HRS-02
	Contratos laborales	HRS-03
	Finalización de la relación laboral	HRS-04
	Gestión de dispositivos móviles	HRS-05
	Acuerdos de Confidencialidad	HRS-06
	Roles / Responsabilidades	HRS-07
	Uso aceptables de la tecnología	HRS-08
	Formación / Concienciación	HRS-09
	Responsabilidad de los Usuarios	HRS-10
	Lugares de trabajo	HRS-11
Gestión de Identidades y Accesos	Acceso a las Herramientas de Auditoría	IAM-01
	Ciclo de vida de las Credenciales / Gestión del Aprovisionamiento	IAM-02
	Acceso a puertos de diagnóstico / configuración	IAM-03

	Políticas y Procedimientos	IAM-04
	Segregación de Tareas	IAM-05
	Restricciones en el acceso al Código fuente	IAM-06
	Acceso por Terceros	IAM-07
	Fuentes de Confianza	IAM-08
	Autorización del Acceso de Usuarios	IAM-09
	Revisiones del Acceso de Usuarios	IAM-10
	Revocación del Acceso de Usuarios	IAM-11
	Credenciales de Identidad (ID) de Usuarios	IAM-12
	Acceso a los programas de utilidades	IAM-13
Seguridad de la Infraestructura y Virtualización	Registros de Auditoría / Detección de Intrusiones.	IVS-01
	Detección de Cambios	IVS-02
	Sincronización de Relojes	IVS-03
	Documentación de los Sistemas de Información	IVS-04
	Gestión - Gestión de las Vulnerabilidades	IVS-05
	Seguridad de la Red	IVS-06
	Bastionado de Sistema Operativo y Controles Básicos	IVS-07
	Entornos de Producción y No-Producción	IVS-08
	Segmentación	IVS-09
	Seguridad de las Máquinas Virtuales (VM) - Protección de los Datos en las migraciones (vMotion)	IVS-10
	Seguridad VMM - Bastionado del Hypervisor	IVS-11
	Seguridad Inalámbrica	IVS-12
	Arquitectura de Red	IVS-13
Interoperabilidad y Portabilidad	API's	IPY-01
	Peticiones de Datos	IPY-02
	Políticas y Legislación	IPY-03
	Protocolos de Red estandarizados	IPY-04
	Virtualización	IPY-05
Seguridad móvil	Anti-Malware	MOS-01
	Tiendas de aplicaciones	MOS-02
	Aplicaciones aprobadas	MOS-03
	Software aprobado para BYOD	MOS-04
	Formación y concienciación	MOS-05
	Servicios basados en la nube	MOS-06
	Compatibilidad	MOS-07
	Idoneidad de dispositivos	MOS-08
	Inventario de dispositivos	MOS-09
	Gestión de dispositivos	MOS-10
	Cifrado	MOS-11
	Jailbreaking y Rooting	MOS-12
	Requisitos legales	MOS-13
	Bloqueo de pantalla	MOS-14
	Sistemas Operativos	MOS-15
	Contraseñas	MOS-16

	Política	MOS-17
	Borrado remoto	MOS-18
	Parches de seguridad	MOS-19
	Usuarios	MOS-20
Gestión de incidentes de seguridad, Localización de evidencias electrónicas, Investigaciones forenses en la nube	Puntos de contacto con las autoridades	SEF-01
	Gestión de incidentes	SEF-02
	Comunicación de incidentes	SEF-03
	Preparaciones legales para la respuesta ante incidentes	SEF-04
	Métricas de la respuesta ante incidentes	SEF-05
Gestión de la cadena de suministro, Transparencia y Responsabilidad	Calidad de datos e Integridad	STA-01
	Comunicación de incidentes	STA-02
	Servicios de red / infraestructura	STA-03
	Evaluaciones internas del proveedor	STA-04
	Acuerdos relativos a la cadena de suministro	STA-05
	Revisión de la gobernanza de la cadena de suministro	STA-06
	Métricas de la cadena de suministro	STA-07
	Evaluación por parte de terceros	STA-08
	Auditorias por parte de terceros	STA-09
Gestión de vulnerabilidades y amenazas	Antivirus / Software malicioso	TVM-01
	Gestión de parches y vulnerabilidades	TVM-02
	Código móvil	TVM-03

Tabla 16. Lista completa de dominios y grupos de controles (v3.0.1).

4.5 Selección de proveedores

Los documentos CAI Questionnaire son obtenidos a través del registro **STAR** desarrollado por la organización CSA. Dicho registro incluye una lista de proveedores o CSP (*Cloud Service Provider*) cuyos documentos se encuentran publicados para la evaluación de sus servicios cloud. Sin embargo, ha sido necesario un análisis del registro de CSPs para determinar los proveedores válidos para el desarrollo de este proyecto.

Para la **selección** de los proveedores se han seguido una serie de criterios. El **primer criterio de selección** se refiere al tipo de documento proporcionado por la empresa. El documento debe ser CAI Questionnaire para poder realizar el análisis de las métricas de seguridad explicado en apartados anteriores. Algunos CSPs proporcionan un certificado de entrada en el registro o el CCM en lugar del CAIQ. Dichos proveedores son excluidos de la selección.

El **segundo criterio** analiza el formato del documento. Para el proyecto se hace uso de documentos en formato .xls/xlsx (Office Open XML) puesto que es posible su procesado automático a través de un programa. Los cuestionarios en formato PDF no son válidos para el procesado.

También existen ficheros CAIQ en formato .docx (Word) que poseen una estructura interna codificada en XML similar a los anteriores. Sin embargo, el número de proveedores con este tipo de formato es reducido en comparación con el resto, por lo que son descartados.

En la Tabla 17 se incluye el tipo, formato y versión del fichero para todos los proveedores disponibles:

CSP	Tipo Metadato	Formato Fichero	Versión
Acer CyberCenter Services Inc.	CAI Questionnaire	xlsx	1.1
Achievers Corporation	Registry Entry	pdf	-
	STAR Certificate	pdf	-
Acquia	CAI Questionnaire	xls	1.1
Adallom	CAI Questionnaire	xlsx	3.0.1
Alibaba Cloud Computing Ltd.	Registry Entry	pdf	-
Amazon AWS	CAI Questionnaire	pdf	-
	PGP Signature	pdf	-
Aria Systems	CAI Questionnaire	xlsx	1.1
Aryaka	CAI Questionnaire	xlsx	1.1
Blackthorn Technologies	CAI Questionnaire	xlsx	1.1
Box.com	CAI Questionnaire	xlsx	1.1
Brainloop	CAI Questionnaire	pdf	3.0.1
BroadBand Tower, Inc.	Registry Entry	pdf	-
	STAR Certificate	pdf	-
CapLinked	CAI Questionnaire	xlsx	1.1
Capriza	CAI Questionnaire	xlsx/pdf	3.0.1
Carbon60 Networks	CAI Questionnaire	xlsx	1.1
CareTower Ltd.	CAI Questionnaire	xlsx	3.0.1
CARI.net	CAI Questionnaire	xlsx	1.1
China Enterprise ICT Solutions Limited	CAI Questionnaire	xlsx	1.1
Chunghwa Telecom	CAI Questionnaire	pdf	1.1
Chunghwa Telecom Co., Ltd	Registry Entry	pdf	-
Cirrity LLC	Registry Entry	pdf	-
Citrix ShareFile	CAI Questionnaire	pdf	2
Clari Inc.	CAI Questionnaire	xls	1.1
Close IT Support T/A	CAI Questionnaire	xlsx	1.1
Cloud Dinamics Inc.	CAI Questionnaire	xlsx	1.1
CloudAlly Ltd.	CAI Questionnaire	xlsx	1.1
CloudSigma AG	CAI Questionnaire	xlsx	1.1
CSC	CAI Questionnaire	pdf	1.1
Cvent, Inc.	CAI Questionnaire	xlsx	1.1
Data Noah GmbH	CAI Questionnaire	xlsx	3.0.1

Develocus, LLC	CAI Questionnaire	xlsx	3.0.1
Digital Sense Hosting	CAI Questionnaire	xlsx	1.1
Dropbox, Inc	CAI Questionnaire	pdf	1.1
EDC Corporation - AIMS Parking	CAI Questionnaire	xlsx	1.1
Egnyte	CAI Questionnaire	xlsx	1.1
Everbridge	CAI Questionnaire	xlsx	3.0.1
Evolve IP	CAI Questionnaire	xlsx	1.1
Exostar LLc	Cloud Controls Matrix	xlsx	3.0
Exponential-e Ltd.	Registry Entry	pdf	-
Falk-Enrich GmbH License12	CAI Questionnaire	xls	1.1
FireHost	CAI Questionnaire	pdf	1.1
HighRadius	CAI Questionnaire	xlsx	1.1
HKT	CAI Questionnaire	xlsx	3.0.1
HP VPC	CAI Questionnaire	docx	1.1
	CAI Questionnaire	pdf	
HP ECS-G	Registry Entry	pdf	-
Hyland	CAI Questionnaire	pdf	1.1
iLand	CAI Questionnaire	xlsx	3.0.1
Intracom Telecom	CAI Questionnaire	xlsx	1.1
Krescendo	CAI Questionnaire	xlsx	1.1
Laconic Security	CAI Questionnaire	xls	1.1
MaaS360 by Fiberlink	Cloud Controls Matrix	pdf	1.3
Microsoft Dynamics CRM Online	Cloud Controls Matrix	docx	-
Microsoft Office 365	Cloud Controls Matrix	docx	1.4
Microsoft Windows Azure	Cloud Controls Matrix	docx	-
MicroStrategy	CAI Questionnaire	xlsx	1.1
Mimecast	CAI Questionnaire	xlsx	1.1
Netskope	CAI Questionnaire	xlsx	1.1
New Century Inforcomm Tech Co., Ltd.	Registry Entry	pdf	-
New Relic	CAI Questionnaire	xlsx	1.1
New World Telecommunications Ltd	CAI Questionnaire	xlsx	3.0.1
NewBase Computer Services Pty Ltd	CAI Questionnaire	xlsx	1.1
Okta Inc.	CAI Questionnaire	xls	1.1
OneLogin, Inc.	CAI Questionnaire	xlsx	3.0.1
OneNet	CAI Questionnaire	xls/pdf	1.1
OVH	CAI Questionnaire	xlsx	2
Peer 1 Hosting	CAI Questionnaire	xlsx	1.1
Perfecto Mobile	CAI Questionnaire	xlsx	3.0.1
Ping Identity	CAI Questionnaire	xlsx	1.1
PIPED BITS CO., LTD.	Registry Entry	pdf	-
	STAR Certificate	pdf	
PODFather Ltd.	CAI Questionnaire	pdf	1.3
Poste Italiane S.P.A.	Cloud Controls Matrix	pdf	1.02
	Registry Entry	pdf	-
	STAR Certificate	pdf	-

Projectplace International	CAI Questionnaire	xlsx	1.1
PT Sigma Cipta Caraka	Registry Entry	pdf	-
Pulsant Limited	Registry Entry	pdf	-
RapidCompute - Division of Cybernet	CAI Questionnaire	xlsx	1.1
Recall Corporation	Cloud Controls Matrix	xlsx	3.0.1
Red Hat OpenShift	CAI Questionnaire	xls	1.1
Ribose	CAI Questionnaire	xlsx	1.1
	Registry Entry	pdf	-
	STAR Certificate	pdf	-
ServiceNow	Cloud Controls Matrix	xlsx	3.0.1
SHI International, Corp.	CAI Questionnaire	xlsx/pdf	1.1
Shibumi	CAI Questionnaire	xlsx	1.1
Skyhigh Networks	CAI Questionnaire	xlsx	1.1
Sliced Tech	CAI Questionnaire	xlsx	1.1
Slovak Telekom	Cloud Controls Matrix	pdf	3.0
SoftLayer	CAI Questionnaire	xlsx	1.1
Solutionary	CAI Questionnaire	xlsx	1.1
StarRez	CAI Questionnaire	xlsx	1.1
Symantec.cloud	CAI Questionnaire	xlsx/pdf	1.1
TechnoArt Corp	Registry Entry	pdf	-
Telecom Italia S.p.a. Hosting Evolutio	CAI Questionnaire	pdf	1.2
Terremark	CAI Questionnaire	xlsx	1.1
Think On Inc.	CAI Questionnaire	xlsx	1.1
Trackyou Ltd	CAI Questionnaire	xlsx	1.1
Varolii Corporation	CAI Questionnaire	pdf	1.1
Virtustream, Inc.	CAI Questionnaire	xlsx	1.1
VMware, Inc	CAI Questionnaire	pdf	1.0
Vocera Communications, Inc.	CAI Questionnaire	xlsx	3.0.1
Websense Inc.	CAI Questionnaire	xlsx	3.0.1
Wipro Technologies	CAI Questionnaire	xlsx	1.1
Zendesk	CAI Questionnaire	xlsx	1.1
Zscaler	CAI Questionnaire	xlsx	3.0.1

Tabla 17. Lista de proveedores con tipo, formato y versión del documento.

El **último criterio** es el más crítico y trata sobre las versiones de los documentos. Como puede observarse en la Tabla 17, los CAIQ se encuentran principalmente en dos versiones: la versión inicial 1.1 y la versión más reciente 3.0.1.

La estructura global de ambas versiones es similar, pues contienen las mismas categorías (Control Group, CGID, controles y estándares), por lo que es posible su integración dentro de la misma ontología. Sin embargo, en el caso de la versión 1.1, existen diferencias en la forma de estructurar los datos en el documento de distintos proveedores bajo esta misma versión.

Se pueden distinguir tres grupos con diferente estructura de tablas para la versión 1.1 Lo contrario ocurre con la versión 3.0.1, donde el consenso que determina la forma de estructurar las tablas se extiende a todos esos proveedores en común.

A continuación se muestra una tabla comparativa (Tabla 18) de las versiones y sub-versiones con el fin de plasmar las diferencias estructurales y justificar la elección de los documentos utilizados.

Características	v3.0.1	v.1.1		
		Grupo 1	Grupo 2	Grupo 3
Estructura ontología	CG, CGID, CID, Estándares	CG, CGID, CID, Estándares	CG, CGID, CID, Estándares	CG, CGID, CID, Estándares
Codificación XML	Sí	Sí	No	Sí
Formato respuestas del cuestionario	Tres columnas marcan la respuesta (SI, NO , No Aplicable)	Una columna contiene la respuesta (SI, NO, N/A)	Una columna contiene la respuesta (SI, NO, N/A)	Una columna contiene un texto que responde la cuestión
Respuestas procesables	Sí	Sí	No	No
Versión CCM para mapeo de dominios	v3.0	v1.1	v1.1	v1.1

Tabla 18. Comparación versiones de CAI Questionnaire.

Como puede observarse en la Tabla 18, todas las versiones pueden ser representadas mediante la misma ontología. No obstante, el campo de respuesta a las preguntas del cuestionario de los documentos del grupo 3 de la versión 1.1 contiene un texto que justifica la respuesta de la pregunta. Dicho texto no puede ser analizado por el procesador de forma directa para extraer si la respuesta es afirmativa, negativa o no aplicable. Por tanto, a pesar de ser el grupo más numeroso, el grupo 3 es descartado.

El resto si contiene una respuesta simple y procesable por el programa (SI, NO o N/A). Los CAIQ del grupo 2 se encuentran en una versión de Excel antigua que no está definida según la estructura de los documentos SpreadsheetML, por lo que no es válida para el procesado XML.

Finalmente, las **versiones elegidas** son la **v3.0.1** y el conjunto de proveedores con **v1.1** correspondiente al grupo 1. Sin embargo, debido a la actualización de los dominios en el desarrollo de la v3.0.1 por la CSA, éstos no coinciden con la versión previa. Por ello es necesario tratar ambos conjuntos independientemente.

La lista definitiva de proveedores utilizados se indica en la Tabla 19:

CSP	Versión
Adallom	v3.0.1
Aryaka	v1.1
Capriza	v3.0.1
Caretower	v3.0.1
DataNoah	v3.0.1
Devellocus	v3.0.1
EDC Corporation	v1.1
Everbridge	v3.0.1
HKT	v3.0.1
iLand	v3.0.1
New World Telecommunications Ltd	v3.0.1
OneLogin	v3.0.1
Peer1	v1.1
Perfecto Mobile	v3.0.1
Zscaler	v3.0.1

Tabla 19. Lista definitiva de proveedores seleccionados.

5 Implementación y Pruebas

Este capítulo se centra en la implementación del diseño analizado en el capítulo anterior. Se detalla el proceso de codificación de los módulos que componen el sistema. También se exponen los resultados de las pruebas de casos de uso que cumplen los requisitos del sistema.

5.1 Ontología

La herramienta Protégé permite la creación de la ontología requerida como un archivo en formato OWL. La ontología es elaborada siguiendo la estructura de categorías del CAIQ, analizada en el anterior capítulo. Por tanto, se crean las siguientes clases: `CAIQ`, `CG`, `CGID`, `CID`, y `Standard`.

La clase `CAIQ` representa el documento en sí y contiene la subclase `CG`, que representa el dominio de los *Control Group*. Esta clase contiene a su vez la subclase `CGID` que define los diferentes *Control Groups*. Por último, la clase `CGID` incluye las subcategorías `CID` y `Standard` que se corresponden con los controles básicos de seguridad y con los estándares de la industria, respectivamente.

Todas las clases están unidas por relaciones jerárquicas de tipo es-subclase-de. Usando la extensión OntoGraf de Protégé se puede visualizar la arquitectura final de la ontología, como puede observarse en la Figura 16:

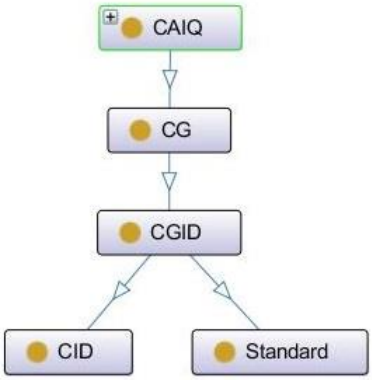

Figura 16. Grafo de clases de la ontología.

Por último, se hace uso de la opción que ofrece el programa para generar el código Java de la ontología con el fin de exportar el código de las clases necesarias en el programa de procesado.

5.2 Procesador de metadatos

El programa procesador de documentos es creado como un proyecto Java en el entorno de desarrollo Eclipse Mars. El objetivo del procesador es el tratamiento de archivos XML (SpreadsheetML) para su conversión en otro formato de datos, en este caso JSON. Para su desarrollo se tienen en cuenta varias alternativas.

5.2.1 Tecnologías utilizadas

Una posible solución sería el uso de las librerías Java proporcionadas por Oracle para el procesamiento de XML, JAXP (*Java API for XML Processing*). JAXP proporciona principalmente dos APIs para el tratamiento de datos XML: DOM y SAX [29].

La tecnología DOM permite obtener una representación en memoria del documento XML. Dicha representación se guarda en un objeto de tipo *Document*, una estructura de árbol que contiene nodos. Cada nodo representa un elemento. Mediante los métodos proporcionados por la API es posible acceder a los elementos del documento a través de sus etiquetas y realizar el procesado del archivo. Se trata de una interfaz sencilla aunque su uso no es recomendable para documentos de gran tamaño, como es el caso de los CAIQ.

A diferencia de la tecnología DOM, SAX no guarda en memoria una instancia del documento, ahorrando en memoria y tiempo de ejecución. En su lugar, el acceso a los elementos se realiza mediante un manejador de eventos. Este método de procesado puede ser usado con grandes documentos, aunque es descartado por su complejidad.

Por tanto, el procesador es implementado usando las librerías de JSON, como alternativa a JAXP. Incluyen métodos para crear objetos JSON a partir de los archivos XML correspondientes a las hojas de cálculo de los CAIQ, como indica la tecnología SpreadsheetML. De esta manera, el procesado consiste en el manejo de objetos JSON que representan los documentos XML y conseguir un objeto JSON final que sigue la estructura definida por la ontología diseñada.

Los archivos XML requeridos son:

- Archivo "*sheet.xml*": representa la hoja de cálculo que contiene la tabla del cuestionario CAI. La estructura de la tabla se expresa mediante elementos de tipo fila (<row>). Cada elemento fila contiene elementos celda (<c>) cuyo valor es un identificador de la cadena de texto que contiene. Este identificador indica la posición de la cadena de texto en el archivo "*sharedStrings.xml*".

- Archivo "*sharedStrings.xml*": contiene la lista de todas las cadenas de texto compartidas por las hojas de cálculo.

5.2.2 Estructura de clases

La estructura de clases se dispone en dos paquetes: uno contiene las interfaces importadas desde Protégé; otro contiene las clases del proyecto. A continuación se muestra el diagrama de clases e interfaces (Figura 17) y una descripción detallada de las clases:

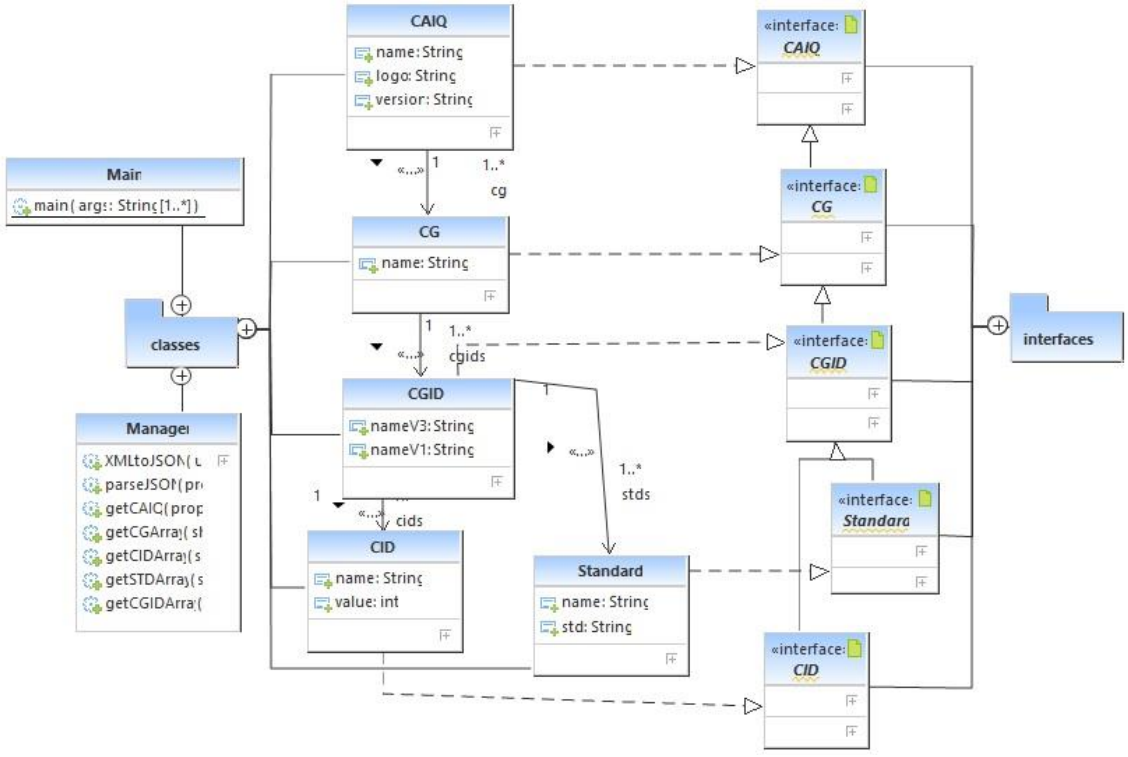

Figura 17. Diagrama UML de clases e interfaces del módulo Procesador.

Por un lado se encuentran las **clases de categorías**. Este grupo de clases representa las categorías presentes en el CAIQ e implementan las entidades definidas en la ontología. Incorporan el código de la ontología importado desde Protégé mediante la implementación de las interfaces. Así pues, se poseen las

clases `CAIQ`, `CG`, `CGID`, `CID` y `Standard` necesarias para la construcción del metadato en formato JSON con la estructura definida:

- Clase "CAIQ": representa el concepto del cuestionario CAI y contiene cuatro atributos. Tres de los atributos son cadenas de texto que indican el nombre del proveedor, la URL del logotipo de la empresa, y la versión del documento, respectivamente. El cuarto atributo es un *array* de objetos CG que simboliza la lista de dominios que incluye el cuestionario.

- Clase "CG": representa un dominio del CAIQ. Está formada por el nombre del dominio y un *array* de CGID que contiene.

- Clase "CGID": simboliza un grupo de controles (CGID). Contiene un *array* de controles (CID) y otro de estándares (Standard). Además, contiene dos atributos de nombre, según la versión del documento. De este modo es posible la integración de ambas versiones bajo la misma ontología.

- Clase "CID": representa un control de seguridad simple. Contiene el nombre del control y un valor asignado en base a la respuesta a la cuestión de ese control: si la respuesta es "SI", se le aplica un valor de 1; si es "NO", un valor de 0; si la respuesta es "No Aplicable" no se aplica ningún valor y el control es ignorado.

- Clase "Standard": indica un estándar de la industria vinculado a un *Control Group*. Contiene el nombre de la familia de estándares y la lista de estándares correspondientes al CG.

Las clases anteriores cuentan con métodos "get" y "set" para acceder y modificar sus atributos, respectivamente. Estos métodos son necesarios para construir los objetos JSON directamente a partir de objetos de estas clases. Esto es debido a que el constructor de objetos JSON proporcionado por la librería detecta los atributos de la clase mediante estos métodos "get" y "set" para construir el objeto JSON con la estructura correcta.

Por otro lado se encuentra la clase "**Manager**". Esta clase contiene los métodos que realizan el procesado. Debido a las diferencias estructurales en las dos versiones, ambas son tratadas de forma independiente. Los métodos principales son los siguientes:

- Método "XMLtoJSON": la función de este método es convertir un archivo XML en formato JSON para permitir su tratamiento mediante las librerías de JSON. Para ello es necesario indicar la ruta de los archivos XML correspondiente a cada proveedor.

- Método “parseJSON”: este método devuelve el objeto JSON final de un CAIQ de un proveedor en el formato de la ontología desarrollada. La obtención del metadato final se realiza mediante una serie de llamadas jerárquicas a métodos internos cuya función es recorrer el CAIQ y estructurar los datos. Dichos métodos construyen las diferentes categorías a medida que son invocados.

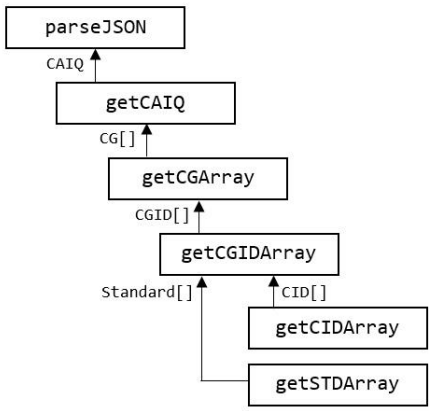

Figura 18. Esquema llamadas a métodos internos.

Por último, la clase “**Main**” que ejecuta el programa procesador. En ella se invoca el método “parseJSON” anterior a través de una instancia de la clase Manager y se establece la conexión con la base de datos para el almacenamiento de los metadatos JSON de los proveedores. Finalmente, tras la conversión se obtiene un objeto JSON con la estructura deseada (Figura 19):

```
{   "name": "Zscaler",
    "logo": "https://www.zscaler.com/images/znew-logo.png",
    "version": "3.0.1",
    "cg": [
        {   "name": "Application & Interface Security"
            "cgids": [
                {   "nameV3": "AIS-01",
                    "nameV1" : "SA-04",
                    "CID": [
                        {   "name": "AIS-01.1",
                            "value": 1
                        }, {...}
                    ]
                    "STDS": [
                        {   "name": "AICPA TSC 2009",
                            "std": "S3.10.0"
                        }, {...}
                    ]
                }, {...}
            ]
        }, {...}
    ]
}
```

Figura 19. Ejemplo de metadato JSON de un proveedor Cloud.

5.3 Base de datos

El sistema de bases de datos NoSQL utilizado es MongoDB. En este proyecto sólo es necesario crear una instancia de base de datos, llamada "TFG", y la colección "CAIQs", donde se almacenan todos los metadatos procesados.

Antes de establecer conexiones con la base de datos, se debe ejecutar el servicio "mongod.exe" que recibe dichas conexiones en el puerto 27017 por defecto.

El acceso a la base de datos tiene lugar a través de dos vías: comunicación con el módulo procesador y con la API del servicio Web. La interacción entre dichos programas y la base de datos es llevada a cabo usando las librerías de MongoDB para Java. Los métodos utilizados para la conexión con la base de datos son los siguientes.

- Constructor "MongoClient('localhost', 27017)": en primer lugar, se debe crear una instancia de un cliente que se conecta con el servicio de MongoDB. Para ello, se indica el host donde se ejecuta y el puerto utilizado para las conexiones.

- Método "getDB('TFG')": obtiene el acceso a la base de datos creada, en este caso "TFG".

- Método "getCollection('CAIQs')": permite acceder a la colección indicada incluida en la base de datos anterior.

- Método "close()": una vez utilizada la base de datos, se debe cerrar la instancia usando este método.

La conexión del procesador con la base de datos se realiza para el almacenamiento de los metadatos en la colección mediante el uso del método "insert()". Previo al almacenamiento de datos nuevos, se utiliza el método "remove()" para eliminar los documentos anteriores.

Por otro lado, la comunicación con la API se basa en consultas personalizadas a la base de datos, mediante el método "find(query, fields)". El argumento "query" indica las condiciones de la consulta y "fields" indica los campos del metadato que se demandan.

5.4 Servicio Web (API REST)

La implementación del servicio web REST que define la API de peticiones es llevaba a cabo mediante un proyecto web con el *framework* JAX-RS (Jersey) integrado en el entorno Eclipse.

Al utilizar el *framework* Jersey es necesario configurar explícitamente el *servlet* en el archivo "web.xml" de la aplicación para el correcto funcionamiento en el contenedor de *servlets* Tomcat. A continuación se muestra un extracto del archivo "web.xml":

```
<web-app>
  <display-name>APIREST</display-name>
  <servlet>
    <servlet-name>Jersey REST Service</servlet-name>
    <servlet-class> org.glassfish.jersey.servlet.ServletContainer
    </servlet-class>
    <init-param>
        <param-name>jersey.config.server.provider.packages
        </param-name>
        <param-value>webservices</param-value>
    </init-param>
  </servlet>
  <servlet-mapping>
    <servlet-name>Jersey REST Service</servlet-name>
    <url-pattern>/rest/*</url-pattern>
  </servlet-mapping>
</web-app>
```

Hay varios aspectos a comentar sobre este archivo de configuración. En primer lugar, se registra el *servlet* de la aplicación que se encarga de recibir y capturar las peticiones RESTful dirigidas a la url de la aplicación indicada (/rest). A continuación, se indica el paquete (webservices) donde se encuentran las clases que deben procesar dichas peticiones. Por último, la URL del *servlet* se constituye de la siguiente manera:

```
http://[dominio]/APIREST/rest/[rutas de las clases y métodos]
```

5.4.1 Estructura de clases

La aplicación se implementa mediante dos clases Java. La clase "**Pet**" incluye la definición de los métodos que atienden las peticiones HTTP a la API. Los métodos se configuran mediante las anotaciones proporcionadas por el framework Jersey.

La clase "**ManagerREST**" incluye los métodos que realizan las tareas de procesado de los metadatos requeridos en las consultas de la clase anterior. De esta manera, en la API se han definido los siguientes métodos que atienden las consultas HTTP:

Petición 1: Lista de proveedores

```
@GET
@Path("/List")
@Produces(MediaType.APPLICATION_JSON)
public String getJSONList()
```

Este método responde a una petición de tipo GET con la lista completa en formato JSON de todos los proveedores de servicios Cloud analizados. La lista contiene el nombre de los diferentes proveedores y la URL del logotipo de la empresa.

La obtención de la lista de proveedores se consigue mediante consultas a los campos de nombre y logo de todos los metadatos almacenados en la base de datos.

Petición 2: Nombres de criterios

```
@GET
@Path("/CritNames")
@Produces(MediaType.APPLICATION_JSON)
public String getJSONCritName(
            @DefaultValue("0") @QueryParam("gran") int granularidad)
```

Este método devuelve los nombres de los criterios o categorías de los metadatos. La consulta HTTP que atiende debe contener un parámetro ("gran") que indique el nivel de granularidad o nivel de detalle deseado. Hay tres niveles de granularidad correspondientes a las tres categorías que estructuran los metadatos CAIQ.

El nivel de granularidad **alta** muestra los nombres correspondientes a los controles de seguridad (**CID**) de los metadatos. El nivel de detalle **medio** da como resultado los nombres de los Control Group (**CGID**) de los CAIQ. Se incluyen los nombres para las versiones 3.0.1 y 1.1. Con el nivel de granularidad **baja** se incluyen los nombres de los criterios correspondientes a los dominios (**CG**) de los metadatos.

Petición 3: Métricas de criterios

```
@GET
@Path("/CritVal")
@Produces(MediaType.APPLICATION_JSON)
public String getJSONCritVal(
            @DefaultValue("0") @QueryParam("gran") int granularidad,
            @DefaultValue("All") @QueryParam("prov") String prov)
```

Este método devuelve como los nombres de los criterios o categorías y los valores asociados a las métricas de seguridad asignadas en el procesado de los documentos. Estas **métricas** proporcionan una **medida de seguridad** basada en la aplicación de los controles de los servicios Cloud de los proveedores. La petición incluye un parámetro que representa el nivel de detalle o granularidad, otro que permite seleccionar un proveedor específico. Si en la petición no se indica ninguno, se devuelve la información para todos los proveedores.

Los valores están asignados a los controles individualmente. Por tanto, para asignar las métricas a los criterios CG y CGID se deben calcular nuevos valores agregados. Dichos valores son calculados como la media de los valores para los criterios aplicables, mediante la siguiente fórmula:

$$\frac{\sum Valores\ de\ los\ controles}{Número\ de\ controles\ aplicables}$$

Con el nivel **alto** de detalle se obtienen los nombres de los controles (**CID**) y sus métricas asociadas, para los proveedores seleccionados. Un valor de 1 representa una respuesta "SI" en el cuestionario CAI, y un valor de 0 una respuesta "NO". Los controles no aplicables no están incluidos en el metadatos, como se detalla en el apartado del programa procesador.

En el nivel **medio** se incluyen los nombres de los Control Group (**CGID**) y sus valores agregados calculados mediante la fórmula anterior.

Por último, el nivel **bajo** de granularidad presenta los nombres de los dominios (**CG**) y los valores agregados de todos los controles que contiene. Es necesario un nuevo cálculo de los valores teniendo en cuenta las métricas calculadas para el criterio Grupos de Controles.

Petición 4: Documento CAIQ completo

```
@GET
@Path("/CAIQ")
@Produces(MediaType.APPLICATION_JSON)
public String getCAIQ(
                @QueryParam("prov") String prov)
```

Este método adicional devuelve el documento CAIQ completo almacenado en la base de datos para un proveedor específico. El proveedor se indica mediante el parámetro "prov" en la petición.

Finalmente, el proyecto API REST es integrado en el servidor Apache Tomcat mediante la exportación del fichero ".war" de la aplicación a la carpeta "webapps".

5.4.2 Dominio no-ip

Para el acceso a los recursos de la API es necesario especificar un dominio en la URI. Dicho dominio se implementa mediante la tecnología no-ip. No-ip es un proveedor de servicios DNS dinámicos que permite la creación de host virtuales mediante el uso de dominios gratuitos. Tras crear una cuenta de usuario, se añade un host virtual vinculado a la IP del servidor web desplegado. El dominio utilizado es: **jose10029.ddns.net**. Por tanto, las rutas de acceso a los recursos de la API quedan definidas de la siguiente manera (Figura 20):

Figura 20. Esquema de rutas de los recursos de la API.

5.5 Resultados de pruebas

En este apartado se realizan las pruebas de validación y de integración de casos de uso mediante un navegador para comprobar el funcionamiento del sistema implementado. Las pruebas consisten en el acceso a todos los recursos disponibles en la API a través de su URI con el fin examinar que el formato y estructura de las respuestas a las peticiones sean correctos. A continuación se muestran las rutas de cada petición y el objeto recibido en la respuesta. Los ejemplos de los objetos JSON se encuentran en formato reducido debido su tamaño original.

5.5.1 Pruebas de casos de uso

En este apartado se realizan las pruebas de los casos de uso y se analiza si el sistema cumple los requisitos indicados en el Capítulo 4.

En primer lugar se realiza la consulta de la lista de proveedores y sus logotipos:

```
http://jose10029.ddns.net/APIREST/rest/pet/List
```


```
{
    "Prov1": {
        "name": "Adallom",
        "logo": "https://www.adallom.com/..../logo--adallom.svg"
    },

    "Prov2": {
        "name": "Capriza",
        "logo": "http://www.capriza.com/..../capriza-logo-blog.png"
    },
    .
    .
    .
    .

    "Prov11": {
        "name": "Perfecto Mobile",
        "logo": "http://www.perfectomobile.com/..../perfecto-mobile.png"
    },
    "Prov12": {
        "name": "Zscaler",
        "logo": "https://www.zscaler.com/..../znew-logo.png"
    },
}
```


Figura 21. Lista de CSPs resultado de la petición.

Esta prueba verifica el cumplimiento del **requisito funcional R-04**, referente a la accesibilidad de la lista de proveedores por parte del usuario.

A continuación, se llevan a cabo las peticiones al recurso que representa los nombres de los diferentes criterios, según los tres niveles de granularidad. Para ello, se debe incluir el parámetro “gran” en la petición:

- Ruta del recurso de los nombres para granularidad alta:

```
http://jose10029.ddns.net/APIREST/rest/pet/CritNames?gran=3
```

```
{"cg": [
    {"cgids": [
        {"CID": [
            {"name": "AIS-01.1"},
            {"name": "AIS-01.2"},
            {"name": "AIS-01.3"},
            {"name": "AIS-01.4"},
            {"name": "AIS-01.5"}
        ]},
        ...
        ...
    ]},
    ...
    ...
    {"cgids": [
        {"CID": [
            {"name": "TVM-01.1"},
            {"name": "TVM-01.2"}
        ]},
        ...
        ...
    ]}
]}
```


Figura 22. Nombres de criterios con granularidad alta (Controles).

- Ruta del recurso de los nombres para granularidad media:

```
http://jose10029.ddns.net/APIREST/rest/pet/CritNames?gran=2
```


```
{"cg": [
    {"cgids": [
        {
            "nameV3": "AIS-01",
            "nameV1": "SA-04"
        },
        {
            "nameV3": "AIS-02",
            "nameV1": "SA-01"
        },
        ...
        ...
    ]},
    {"cgids": [
        {
            "nameV3": "TVM-01",
            "nameV1": "IS-21"
        },
        ...
        ...
    ]}
]}
```


Figura 23. Nombre de criterios con granularidad media (Grupos de Controles).

- Ruta del recurso de los nombres para granularidad baja:

```
http://jose10029.ddns.net/APIREST/rest/pet/CritNames?gran=1
```


```
{"cg": [
    {"name": "Application & Interface Security"},
    {"name": "Audit Assurance & Compliance"},
    {"name": "Business Continuity Management & Operational Resilience"},
    {"name": "Change Control & Configuration Management"},
    {"name": "Data Security & Information Lifecycle Management"},
    {"name": "Datacenter Security"},
    {"name": "Encryption & Key Management"},
    {"name": "Governance and Risk Management"},
    {"name": "Human Resources"},
    {"name": "Identity & Access Management"},
    {"name": "Infrastructure & Virtualization Security"},
    {"name": "Interoperability & Portability"},
    {"name": "Mobile Security"},
    {"name": "Security Incident Management, E-Discovery & Cloud Forensics"},
    {"name": "Supply Chain Management, Transparency and Accountability"},
    {"name": "Threat and Vulnerability Management"}
]}
```


Figura 24. Nombre de criterios con granularidad baja (Dominios).

Este caso de uso cumple el **requisito funcional R-05** relativo a la disponibilidad de la lista de los nombres de los criterios según distintos niveles de detalle.

A continuación, se realizan las consultas para obtener las métricas asociadas a cada criterio. Al igual que la petición anterior, se debe indicar el nivel de detalle mediante el parámetro “gran”. En cuanto al parámetro “prov”, se ha elegido como ejemplo el proveedor Devellocus:

- Ruta del recurso de las métricas para granularidad alta:

```
http://jose10029.ddns.net/APIREST/rest/pet/CritVal?gran=3&prov=Devellocus
```

```
{   "Prov1": {
        "name": "Develloc us",
        "cg": [
            {"cgids": [
                {"CID": [
                    {   "name": "AIS-01.1",
                        "value": 1
                    },
                    {   "name": "AIS-01.2",
                        "value": 1
                    },
                    ...
                    ...
                ]},
                ...
                ...
            ]},
            ...
            ...
            {"cgids": [
                {"CID": [
                    {   "name": "TVM-01.1",
                        "value": 1
                    },
                    {   "name": "TVM-01.2",
                        "value": 1
                    }
                ]},
                ...
                ...
            ]}
        ],
    }
}
```


Figura 25. Métricas de criterios con granularidad alta (Controles).

- Ruta del recurso de las métricas para granularidad media:

```
http://jose10029.ddns.net/APIREST/rest/pet/CritVal?gran=2&prov=Devellocus
```


```
{   "Prov1": {
        "name": "Devellocus",
        "cg": [
            {"cgids": [
                {   "nameV3": "AIS-01",
                    "nameV1": "SA-04",
                    "value": 1
                },
                {   "nameV3": "AIS-02",
                    "nameV1": "SA-01",
                    "value": 0.5
                },
                ...
                ...
            ]},
            ...
            ...
            {"cgids": [
                {   "nameV3": "TVM-01",
                    "nameV1": "IS-21",
                    "value": 1
                },
                {   "nameV3": "TVM-02",
                    "nameV1": "IS-20",
                    "value": 1
                },
                {   "nameV3": "TVM-03",
                    "nameV1": "SA-15",
                    "value": 1
                }
            ]}
        ],

    }
}
```


Figura 26. Métricas de criterios con granularidad media (Grupos de Controles).

- Ruta del recurso de las métricas para granularidad baja:

```
http://jose10029.ddns.net/APIREST/rest/pet/CritVal?gran=1&prov=Devellocus
```


```
{   "Prov1": {
        "name": "Devellocus",
        "cg": [
            {   "name": "Application & Interface Security",
                "value": 0.75
            },
            {   "name": "Audit Assurance & Compliance",
                "value": 0.25
            },
            {   "name": "Business Continuity Management & Operational Resilience",
                "value": 0.3181818
            },
            ...
            ...
            {
                "name": "Threat and Vulnerability Management",
                "value": 1
            }
        ],

    }
}
```


Figura 27. Métricas de criterios con granularidad baja (Dominios).

Los resultados obtenidos se corresponden con los metadatos procesados en el apartado de implementación y el acceso a los recursos es realizado correctamente. Para acceder a la lista completa de todos los proveedores y sus métricas se debe omitir el parámetro "prov" al realizar la petición. Este caso de uso cumple el **requisito funcional R-06**.

Por último, se presenta el caso de uso de la petición para obtener el documento CAIQ completo para un proveedor específico, en este ejemplo el CSP Devellocus, que satisface el **requisito funcional R-07** de información adicional:

```
http://jose10029.ddns.net/APIREST/rest/pet/CAIQ?prov=Devellocus
```

```
{   "name": "Develocus",
    "logo": "http://www.develocus.com/....logo-icon.png",
    "version": "3.0.1",
    "cg": [
        {  "name": "Application & Interface Security",
           "cgids": [
               {   "nameV3": "AIS-01",
                   "nameV1": "SA-04",
                   "STDS": [
                       {   "std": "S3.10.0",
                           "name": "AICPA TSC 2009"
                       }, {...}
                   ],
                   "CID": [
                       {   "name": "AIS-01.1",
                           "value": 1
                       }, {...}
                   ]
               }, {...}
           ],
        }, {...},
        {   "name": "Threat and Vulnerability Management",
           "cgids": [
               {   "nameV3": "TVM-01",
                   "nameV1": "IS-21",
                   "STDS": [
                       {...}
                   ],
                   "CID": [
                       {...}
                   ]
               },
           ],
        }
    ],
}
```


Figura 28. Documento CAIQ completo en formato JSON.

También se han realizado pruebas de integración desde una aplicación web correspondiente al proyecto complementario mencionado en el capítulo de introducción. Dicha aplicación implementa una interfaz de usuario para la comparación de los distintos servicios de los proveedores Cloud. Para realizar la comparación, la aplicación accede a los recursos desplegados en este proyecto, verificando el correcto funcionamiento del sistema de gestión de metadatos de seguridad.

Para realizar dichas pruebas, la aplicación integra las diferentes categorías de controles de seguridad de la CSA analizados en este proyecto. Además, es necesario gestionar la información de los logotipos de las empresas proveedoras, de manera que sea utilizada en la interfaz de usuario de la aplicación Web.

6 Gestión del Proyecto y Presupuesto

En este capítulo se presenta la planificación del proyecto, indicando las distintas fases que se han atravesado en el desarrollo y el tiempo empleado en cada una ellas mediante un diagrama de Gantt. También se analizan los costes de los recursos empleados en el proyecto, plasmados en el presupuesto.

6.1 Planificación y fases

La realización del Trabajo Fin de Grado puede considerarse comprendida desde el mes enero, fecha de asignación del proyecto, hasta el mes de septiembre. Debido a la finalización del curso académico existe un periodo de tiempo en el mes de mayo en el cual no se pudo realizar ninguna tarea. Se distinguen las siguientes fases en el desarrollo del proyecto:

- Fase inicial: comprende el planteamiento inicial del proyecto y el análisis de la documentación de las tecnologías necesarias.

- Diseño: consiste en la definición de los requisitos del sistema y la arquitectura de los módulos que lo componen, la elaboración de la ontología y la selección de los proveedores Cloud.

- Implementación: en esta fase tiene lugar la instalación del entorno de desarrollo utilizado (IDE Eclipse, base de datos y servidor web) y el proceso de codificación de los diferentes módulos del sistema.

- Pruebas: se realizan las pruebas de validación e integración pertinentes para comprobar el funcionamiento del sistema.

- Documentación: fase final que se corresponde con la elaboración de la memoria de trabajo.

Además de las fases indicadas, durante el desarrollo ha tenido lugar una fase de seguimiento del trabajo compuesta por una serie de reuniones con las tutoras con el fin de comprobar y verificar los avances en el desarrollo del proyecto.

El diagrama de Gantt mostrado en la Figura 29 representa el tiempo dedicado a las tareas correspondientes a las fases del desarrollo del proyecto indicadas anteriormente. Las fases se dividen a su vez en sub-tareas, mostrando las relaciones de secuenciación entre ellas. Para cada una de las fases se indica la fecha de inicio, fecha de finalización y la duración en días de las tareas.

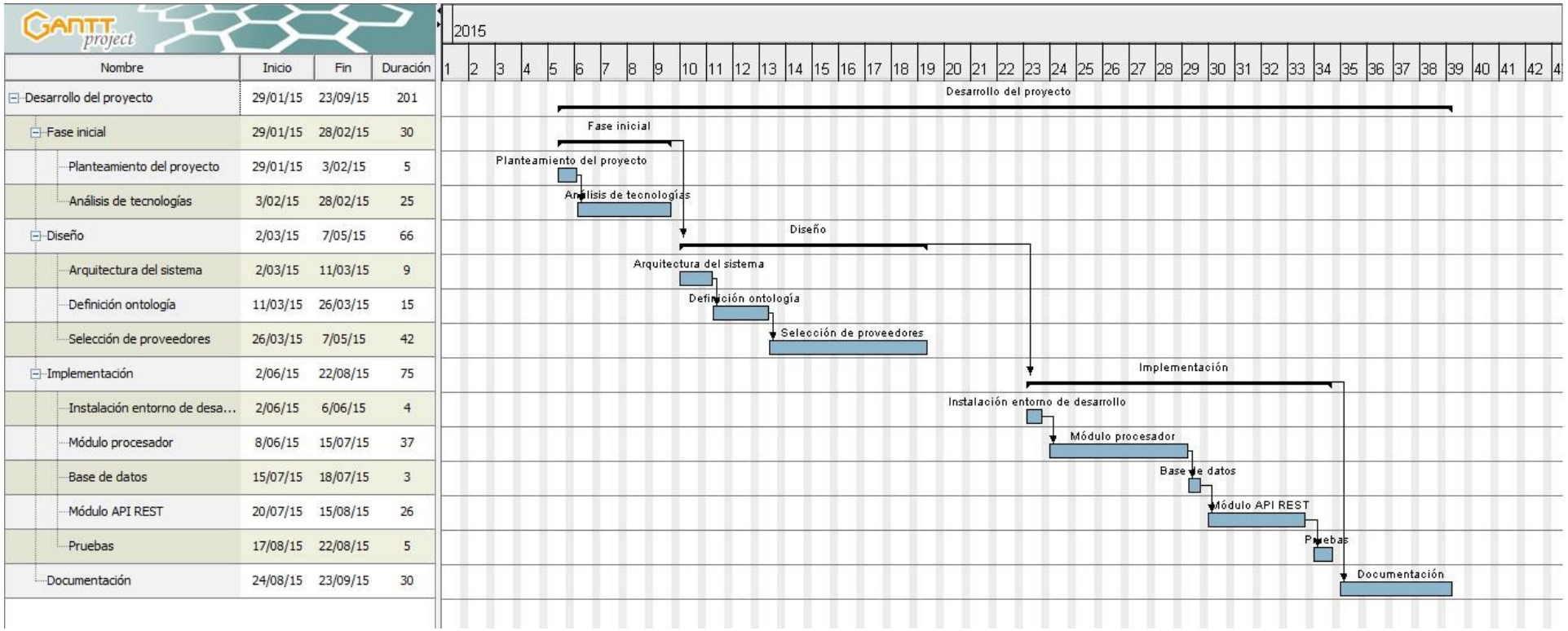

Figura 29. Diagrama de Gantt.

6.2 Presupuesto

Los costes contemplados en el presupuesto se desglosan de la siguiente manera:

COSTES MATERIALES				
Concepto	**Coste (€)**	**Dedicación (meses)**	**Periodo de depreciación (meses)**	**Coste imputable (€)**
PC portátil	450,00	7	48	65,62
Microsoft Office 2013	119,00	7	48	17,35
			TOTAL	**79,97**

Tabla 20. Costes materiales del proyecto.

La duración del proyecto es de 7 meses (201 días) y el periodo de depreciación considerado para los recursos materiales utilizados es de 48 meses. En base a dicha información, el coste de los recursos materiales imputable al proyecto se calcula mediante la siguiente fórmula:

$$Coste\ imputable = \frac{Dedicación}{Periodo\ depreciación} \cdot Coste$$

COSTES DE PERSONAL			
Concepto	**Dedicación (horas)**	**Coste por hora (€)**	**Coste total (€)**
Director de Proyecto	105	30	3.150,00
Analista	75	18	1.350,00
Diseñador	132	18	2.376,00
Programador	225	18	4.050,00
Documentalista	90	18	1.620,00
		TOTAL	**12.546,00**

Tabla 21. Costes de personal del proyecto.

Los costes de personal se calculan según el tiempo dedicado a cada fase del proyecto y a los costes estimados relacionados con dichas tareas.

COSTE TOTAL	
Concepto	**Coste (€)**
Material	79,97
Personal	12.546,00
TOTAL	**12.625,97**

Tabla 22. Presupuesto total del proyecto.

7 Conclusions

This project focuses on the development of a part of a joint project aimed at creating a web application that provides help to customers and companies in the adoption of cloud solutions by analysing security services and comparing several cloud providers.

Concretely, this project has focused on the part of the development of internal system that manages the security metrics needed in the Web application. The system has been successfully implemented by achieving the goals outlined in Chapter 1:

- The Security controls of cloud services have been analysed, through CAIQ documents of providers registered in CSA STAR.
- The CAIQ metadata structure has been analysed to elaborate a common ontology.
- The system implemented a Java program, which parses CAIQ metadata into a JSON format with the structure defined by ontology, managing security metrics.
- The system implemented an Apache web server which integrates the API to access to metadata by the web application developed in the complementary project.
- A NoSQL database (MongoDB), which stores JSON metadata, has been installed.

The objectives have been verified by validations tests, indicated in Chapter 5, and integration testing from the web application implemented in the complementary project.

One important point for the achievements of the objectives has been the monitoring work by tutors, who have resolved the questions rose during the project.

The following section presents the problems encountered and skills gained in the project.

7.1 Problems encountered

During the system development several difficulties have arisen, but these problems have been solved.

One problem is due to the existence of CSPs that do not include a CAIQ document in CSA STAR. Instead, these providers include other files that can't be processed. As a result, there CSPs have been discarded.

However, the main problems encountered are the differences in the versions of the CAI Questionnaires regarding the structure of its data, as detailed in Chapter 4. These differences have increased the difficulties of programming process for both document versions.

Through these problems I have improved my programming skills and my ability to analyse. Also, I learned to use technology that had not previously used, as ontologies tool Protégé or NoSQL database MongoDB, increasing my knowledge and skills to face the future.

7.2 Future Works

As stated in the previous point, the developed system satisfies the initial aims. However, the system can be improved to achieve new goals. Then several future lines of work to implement these possible improvements are presented:

First, the developed system is capable of processing CAIQ documents v3.0.1 and a particular group of v1.1. The first **future work** would be **the processing of all CAIQ documents v1.1**, including all sub-groups. To do this, it should be analysed in depth correspondences between versions 3.0.1 and 1.1 for the integration of the two versions in the same application. Thus, the number of available cloud service providers would increase considerably, improving the quality and usefulness of this tool.

Secondly, another **future work** would be to implement a system that automatically obtains the metadata from the CSA STAR registry. The system could be implemented using **Selenium**, a software testing framework for web applications that can record and play back actions performed by the user through a browser as Firefox. Using this tool, it would be possible to record the sequence of actions of

CAIQ documents downloading from the STAR registry and, later, play them in the application for auto get.

Another **future work** is the implementation of **new functions in the API** that provide access to new resources and information of security metadata. Thus, usability and usefulness of the application and the user experience would be improved.

In this project, the information of industry standards contained in CAI Questionnaire (Annex C) is not completely processed. These standards are managed in the system as additional data and stored as a simply string, but it is a very valuable information in the process of cloud service adoption. So, one of the new functions would be the **explicit management** of these **standard** information.

The last proposed **future work** is the **automatic management** of companies' **logos**. As stated in Chapter 5, these logos are needed by the user interface implemented in the Web application of complementary project. The idea is to get automatically these logos from CSA website. To do this, it is necessary a mechanism provided by CSA which allows to access these data from the STAR registry of providers.

8 Glosario de términos

API: *Application Programming Interface*, conjunto de funciones, subrutinas y herramientas que permite la interacción entre componentes software.

CAIQ: *Consensus Assessment Initiative Questionnaire*, documento acerca de los controles de seguridad de servicios Cloud.

CCM: *Cloud Controls Matrix*, matriz de controles de referencia que incorpora las especificaciones para la seguridad de los servicios Cloud.

Cloud: abreviatura que hace referencia al *Cloud Computing* o tecnología en la nube.

CSA: *Cloud Security Alliance*, organización sin ánimo de lucro dedicada a promover la investigación sobre las mejores prácticas para ofrecer garantías de seguridad en Cloud Computing.

CSP: *Cloud Service Provider*, proveedor de servicios Cloud.

Framework: marco de aplicación orientado a la reutilización de componentes software para el desarrollo de aplicaciones.

HTTP: *HiperText Transfer Protocol*, protocolo de transferencia de información utilizado en la web.

IaaS: *Infrastructura as a Service*, modelo Cloud de infraestructura informática como servicio.

Interfaz DOM: *Document Object Model*, API de la librería JAXP para el procesamiento de datos XML mediante la representación en memoria del documento XML

Interfaz SAX: *Simple API for XML*, API de la librería JAXP para el procesamiento XML mediante el manejo de eventos.

JAX-RS: *Java API for RESTful Web Services*, es un framework que permite desarrollar servicios web RESTful.

JAXP: *Java API for XML Processing*, librerías Java para el procesamiento de XML.

JSON: *JavaScript Object Notation*, formato ligero para el intercambio de datos.

JSP: *JavaServer Pages*, tecnología software para la creación de páginas web dinámicas basadas en HTML y XML.

NoSQL: *Not only SQL*, sistemas de bases de datos que difieren del modelo clásico de gestión de bases de datos relacionales.

OWL: *Web Ontology Language*, lenguaje de marcado para publicar y compartir datos de ontologías.

PaaS: *Platform as a Service*, modelo Cloud de plataformas informáticas para el desarrollo de aplicaciones, como servicio.

Plug-in: módulo software que añade una funcionalidad o nueva característica a un sistema.

RDF: *Resource Description Framework*, lenguaje para la especificación de metadatos basado en XML.

REST: *REpresentational State Transfer*, estilo de arquitectura software para sistemas hipermedia distribuidos, como la web, basado en el uso del protocolo HTTP.

SaaS: *Software as a Service*, modelo *Cloud* de aplicaciones software como servicio.

Servlet: módulo basado en Java que extiende las capacidades de petición y respuesta de un servidor.

SOAP: *Simple Object Access Protocol*, protocolo estándar que permite la interacción entre procesos mediante el intercambio de datos XML.

URI: *Universal Resource Identifier*, cadena de caracteres que identifica un recurso en la web.

W3C: *World Wide Web Consortium*, consorcio internacional que produce recomendaciones para la *World Wide Web*.

WSDL: *Web Service Description Language*, formato XML para la descripción de servicios web.

XML: *eXtensible Markup Language*, lenguaje de marcado para el almacenamiento de datos de forma legible.

Bibliografía

[1] Lamarca Lapuente, M. J. 2013. Hipertexto, el nuevo concepto de documentos en la cultura de la imagen. Ontologías. http://www.hipertexto.info/documentos/ontologias.htm

[2] Sánchez López, S. E. 2007. Modelo de indexación de formas en sistemas VIR basado en ontologías. Capítulo 4: Ontologías y su representación jerárquica. http://catarina.udlap.mx/u_dl_a/tales/documentos/mcc/sanchez_l_se/capitulo4.pdf

[3] Barrios Núñez, J. M. 2006. Catalogación y búsqueda semántica en un sitio web. http://users.dcc.uchile.cl/~jbarrios/catalogo/tesis.pdf

[4] Lamarca Lapuente, M. J. 2013. Hipertexto, el nuevo concepto de documentos en la cultura de la imagen. RDF. http://www.hipertexto.info/documentos/rdf.htm

[5] World Wide Web Consortium (W3C). 2004. OWL Web Ontology Language - Overview. http://www.w3.org/TR/2004/REC-owl-features-20040210/

[6] Rouse, M. 2011. Cloud Security Alliance (CSA) definition. http://searchcloudsecurity.techtarget.com/definition/Cloud-Security-Alliance-CSA

[7] National Institute of Standards and Technology (NIST). 2011. The NIST Definition of Cloud Computing. http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf

[8] Cloud Security Alliance. 2015. Research. https://cloudsecurityalliance.org/research/

[9] Kelley, D. 2013. Understanding the CSA Cloud Controls Matrix and CAIQ. http://searchcloudsecurity.techtarget.com/feature/Understanding-the-CSA-Cloud-Controls-Matrix-and-CAIQ

[10] Sánchez, M. A. 2014. Seguridad y Transparencia de los proveedores cloud: la certificación STAR. https://technologyincontrol2.wordpress.com/2014/03/19/seguridad-y-transparencia-de-los-proveedores-cloud-la-certificacion-star/

[11] Instituto Nacional de Ciberseguridad. 2015. CSA STAR. https://www.incibe.es/empresas/Haz_negocios_con_confianza/Csa_Star

[12] Cloud Security Alliance. 2015. CSA Security, Trust & Assurance Registry (STAR) https://cloudsecurityalliance.org/star/

[13] W3C España. Guía Breve de Servicios Web http://www.w3c.es/Divulgacion/GuiasBreves/ServiciosWeb

[14] Navarro Marset, R. 2006. Modelado, Diseño e Implementación de Servicios Web. http://users.dsic.upv.es/~rnavarro/NewWeb/docs/RestVsWebServices.pdf

[15] Fernández, A. 2013. Servicios web RESTful con HTTP. Parte I: Introducción y bases teóricas. http://www.adwe.es/general/colaboraciones/servicios-web-restful-con-http-parte-i-introduccion-y-bases-teoricas

[16] Álvarez Caules, C. 2013. Introducción a Servicios REST. http://www.arquitecturajava.com/servicios-rest/

[17] JSON.org. 2015. Introducción a JSON. http://json.org/json-es.html

[18] World Wide Web Consortium (W3C). 2015. Protégé. https://www.w3.org/2001/sw/wiki/Protege

[19] Edu4Java. 2015. Que es un contenedor de servlets. Instalación Apache Tomcat. http://www.edu4java.com/es/servlet/servlet1.html

[20] The Apache Software Foundation. 2014. Apache Tomcat 8. Introduction. https://tomcat.apache.org/tomcat-8.0-doc/introduction.html

[21] Jendrock, E., Cervera-Navarro, R., Evans, I., Gollapudi, D., Haase, K., Markito, W., Srivathsa, C. 2013. The Java EE 6 Tutorial. Volumen 1. http://docs.oracle.com/javaee/6/tutorial/doc/

[22] Wiesel, J. 2013. MongoDB desde cero. http://codehero.co/series/mongodb-desde-cero.html

[23] Fernández, R. 2014. MongoDB: qué es, cómo funciona y cuando podemos usarlo (o no). http://www.genbetadev.com/bases-de-datos/mongodb-que-es-como-funciona-y-cuando-podemos-usarlo-o-no

[24] Ross, D. 2007. How to Leverage an API for Conferencing. http://money.howstuffworks.com/business-communications/how-to-leverage-an-api-for-conferencing1.htm

[25] Microsoft. 2013. About Open XML SDK 2.5 for Office. https://msdn.microsoft.com/ES-ES/library/office/bb456487.aspx

[26] The Apache Software Foundation. 2004. Apache Software License 2.0. http://www.apache.org/licenses/LICENSE-2.0

[27] GNU Operative System. 2007. GNU Affero General Public License. http://www.gnu.org/licenses/agpl-3.0.html

[28] Open Source Initiative. 2015. The BSD 2-Clause License. http://opensource.org/licenses/bsd-license.php

[29] Oracle. Java API for XML Processing (JAXP). 2015. The Java Tutorials. https://docs.oracle.com/javase/tutorial/jaxp/

Anexos

A continuación se muestran los anexos de la memoria. En el anexo A muestra el esquema RDF/XML completo de la ontología desarrollada. Los anexos B y C muestran el documento CAIQ para un proveedor concreto. Debido al tamaño del documento se ha divido en dos anexos: anexo de controles y anexo de estándares.

Anexo A: Esquema RDF/XML ontología

```
<?xml version="1.0"?>

<!DOCTYPE rdf:RDF [
    <!ENTITY owl "http://www.w3.org/2002/07/owl#" >
    <!ENTITY xsd "http://www.w3.org/2001/XMLSchema#" >
    <!ENTITY rdfs "http://www.w3.org/2000/01/rdf-schema#" >
    <!ENTITY rdf "http://www.w3.org/1999/02/22-rdf-syntax-ns#" >
]>

<rdf:RDF xmlns="http://www.semanticweb.org/pc/ontologies/2015/3/untitled-
                ontology-16#"
     xml:base="http://www.semanticweb.org/pc/ontologies/2015/3/untitled-
                ontology-16"
     xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#"
     xmlns:owl="http://www.w3.org/2002/07/owl#"
     xmlns:xsd="http://www.w3.org/2001/XMLSchema#"
     xmlns:rdfs="http://www.w3.org/2000/01/rdf-schema#">
    <owl:Ontology rdf:about="http://www.semanticweb.org/TFG/CAIQOntology"/>

    <!--
    ////////////////////////////////////////////////////////////////////////
    //
    // Object Properties
    //
    ////////////////////////////////////////////////////////////////////////
     -->

    <!-- http://www.semanticweb.org/TFG/CAIQOntology#hasCategory -->

    <owl:ObjectProperty
    rdf:about="http://www.semanticweb.org/TFG/CAIQOntology#hasCategory">
        <rdfs:domain
        rdf:resource="http://www.semanticweb.org/TFG/CAIQOntology#CAIQ"/>
    </owl:ObjectProperty>
```

```
<!-- http://www.semanticweb.org/TFG/CAIQOntology#hasControl -->

<owl:ObjectProperty
rdf:about="http://www.semanticweb.org/TFG/CAIQOntology#hasControl">
    <owl:propertyDisjointWith
    rdf:resource="http://www.semanticweb.org/TFG/CAIQOntology#hasStandar
    ds"/>
    <rdfs:subPropertyOf
    rdf:resource="http://www.semanticweb.org/TFG/CAIQOntology#hasSubcate
    gory"/>
</owl:ObjectProperty>

<!-- http://www.semanticweb.org/TFG/CAIQOntology#hasStandards -->

<owl:ObjectProperty
rdf:about="http://www.semanticweb.org/TFG/CAIQOntology#hasStandards">
    <rdfs:subPropertyOf
    rdf:resource="http://www.semanticweb.org/TFG/CAIQOntology#hasSubcate
    gory"/>
</owl:ObjectProperty>

<!-- http://www.semanticweb.org/TFG/CAIQOntology#hasSubcategory -->

<owl:ObjectProperty
rdf:about="http://www.semanticweb.org/TFG/CAIQOntology#hasSubcategory">
    <rdfs:subPropertyOf
    rdf:resource="http://www.semanticweb.org/TFG/CAIQOntology#hasCategor
    y"/>
</owl:ObjectProperty>

<!-- http://www.semanticweb.org/TFG/CAIQOntology#isCategoryOf -->

<owl:ObjectProperty
rdf:about="http://www.semanticweb.org/TFG/CAIQOntology#isCategoryOf">
    <rdfs:range
    rdf:resource="http://www.semanticweb.org/TFG/CAIQOntology#CAIQ"/>
    <owl:inverseOf
    rdf:resource="http://www.semanticweb.org/TFG/CAIQOntology#hasCategor
    y"/>
</owl:ObjectProperty>

<!-- http://www.semanticweb.org/TFG/CAIQOntology#isControlOf -->

<owl:ObjectProperty
rdf:about="http://www.semanticweb.org/TFG/CAIQOntology#isControlOf">
    <owl:inverseOf
    rdf:resource="http://www.semanticweb.org/TFG/CAIQOntology#hasControl
    "/>
    <owl:propertyDisjointWith
    rdf:resource="http://www.semanticweb.org/TFG/CAIQOntology#isStandard
    Of"/>
    <rdfs:subPropertyOf
    rdf:resource="http://www.semanticweb.org/TFG/CAIQOntology#isSubcateg
    oryOf"/>
</owl:ObjectProperty>
```

```
<!-- http://www.semanticweb.org/TFG/CAIQOntology#isStandardOf -->

<owl:ObjectProperty
rdf:about="http://www.semanticweb.org/TFG/CAIQOntology#isStandardOf">
    <owl:inverseOf
    rdf:resource="http://www.semanticweb.org/TFG/CAIQOntology#hasStandar
    ds"/>
    <rdfs:subPropertyOf
    rdf:resource="http://www.semanticweb.org/TFG/CAIQOntology#isSubcateg
    oryOf"/>
</owl:ObjectProperty>

<!-- http://www.semanticweb.org/TFG/CAIQOntology#isSubcategoryOf -->

<owl:ObjectProperty
rdf:about="http://www.semanticweb.org/TFG/CAIQOntology#isSubcategoryOf">
    <owl:inverseOf
    rdf:resource="http://www.semanticweb.org/TFG/CAIQOntology#hasSubcate
    gory"/>
    <rdfs:subPropertyOf
    rdf:resource="http://www.semanticweb.org/TFG/CAIQOntology#isCategory
    Of"/>
</owl:ObjectProperty>

<!—
///////////////////////////////////////////////////////////////////////
//
// Classes
//
///////////////////////////////////////////////////////////////////////
 -->

<!-- http://www.semanticweb.org/TFG/CAIQOntology#CAIQ -->

<owl:Class
rdf:about="http://www.semanticweb.org/TFG/CAIQOntology#CAIQ"/>


<!-- http://www.semanticweb.org/TFG/CAIQOntology#CG -->

<owl:Class rdf:about="http://www.semanticweb.org/TFG/CAIQOntology#CG">
    <rdfs:subClassOf
     rdf:resource="http://www.semanticweb.org/TFG/CAIQOntology#CAIQ"/>
</owl:Class>


<!-- http://www.semanticweb.org/TFG/CAIQOntology#CGID -->

<owl:Class rdf:about="http://www.semanticweb.org/TFG/CAIQOntology#CGID">
    <rdfs:subClassOf
     rdf:resource="http://www.semanticweb.org/TFG/CAIQOntology#CG"/>
</owl:Class>
```

```
    <!-- http://www.semanticweb.org/TFG/CAIQOntology#CID -->

    <owl:Class rdf:about="http://www.semanticweb.org/TFG/CAIQOntology#CID">
        <rdfs:subClassOf
         rdf:resource="http://www.semanticweb.org/TFG/CAIQOntology#CGID"/>
    </owl:Class>


    <!-- http://www.semanticweb.org/TFG/CAIQOntology#Standard -->

    <owl:Class
    rdf:about="http://www.semanticweb.org/TFG/CAIQOntology#Standard">
        <rdfs:subClassOf
         rdf:resource="http://www.semanticweb.org/TFG/CAIQOntology#CGID"/>
    </owl:Class>

</rdf:RDF>


<!-- Generated by the OWL API (version 3.5.1) http://owlapi.sourceforge.net
-->
```

Anexo B: CAIQ (I). Controles

Debido al tamaño de la Tabla 23, se ha obviado parte de las descripciones más extensas de los controles.

Control Group	CGID	CID	Control Specification	Consensus Assessment Questions	Consensus Assessment Answers			Notes
					Yes	No	NA	
Application & Interface Security *Application Security*	AIS-01	AIS-01.1	**Applications and programming interfaces (APIs) shall be designed, developed, deployed and tested in accordance with leading industry standards (e.g., OWASP for web applications) and adhere to applicable legal, statutory, or regulatory compliance obligations.**	Do you use industry standards (Build Security in Maturity Model [BSIMM] benchmarks, Open Group ACS Trusted Technology Provider Framework, NIST, etc.) to build in security for your Systems/Software Development Lifecycle (SDLC)?	Yes			
		AIS-01.2		Do you use an automated source code analysis tool to detect security defects in code prior to production?	Yes			
		AIS-01.3		Do you use manual source-code analysis to detect security defects in code prior to production?	Yes			
		AIS-01.4		Do you verify that all of your software suppliers adhere to industry standards for Systems/Software Development Lifecycle (SDLC) security?	Yes			
		AIS-01.5		(SaaS only) Do you review your applications for security vulnerabilities and address any issues prior to deployment to production?	Yes			
Application & Interface Security *Customer Access Requirements*	AIS-02	AIS-02.1	**Prior to granting customers access to data, assets, and information systems, (removed all) identified security, contractual, and regulatory requirements for customer access shall be addressed.**	Are all identified security, contractual and regulatory requirements for customer access contractually addressed and remediated prior to granting customers access to data, assets and information systems?	Yes			
		AIS- 02.2		Are all requirements and trust levels for customers' access defined and documented?		No		This is performed on a per-customer basis
Application & Interface Security *Data Integrity*	AIS-03	AIS-03.1	**Data input and output integrity routines (i.e., reconciliation and edit checks) shall be implemented for application interfaces and databases to prevent manual or systematic processing errors, corruption of data, or misuse.**	Are data input and output integrity routines (i.e., reconciliation and edit checks) implemented for application interfaces and databases to prevent manual or systematic processing errors or corruption of data?	Yes			checks are performed in the application interface
Application &	AIS-04	AIS-04.1	**Policies and procedures shall be established and**	Is your Data Security Architecture designed using an industry standard (e.g., CDSA,	Yes			Adallom's data security

Interface Security *Data Security / Integrity*			**maintained in support of data security to include (confidentiality, integrity and availability) across multiple system interfaces, jurisdictions and business functions to prevent improper disclosure, alternation, or destruction.**	MULITSAFE, CSA Trusted Cloud Architectural Standard, FedRAMP, CAESARS)?				architecture is designed in accordance with the relevant standards, including CSA and FedRAMP.
Audit Assurance & Compliance *Audit Planning*	AAC-01	AAC-01.1	**Audit plans shall be developed and maintained to address business process disruptions. Auditing plans shall focus on reviewing the effectiveness of the implementation of security operations. All audit activities must be agreed upon prior to executing any audits.**	Do you produce audit assertions using a structured, industry accepted format (e.g., CloudAudit/A6 URI Ontology, CloudTrust, SCAP/CYBEX, GRC XML, ISACA's Cloud Computing Management Audit/Assurance Program, etc.)?	Yes			Adallom is audited according to a number of standards including SOC2 type 2 and CSA TRUST
Audit Assurance & Compliance *Independent Audits*	AAC-02	AAC-02.1	**Independent reviews and assessments shall be performed at least annually to ensure that the organization addresses nonconformities of established policies, standards, procedures and compliance obligations.**	Do you allow tenants to view your SOC2/ISO 27001 or similar third-party audit or certification reports?	Yes			Reports are available to customers and prospects under a non-disclosure agreement (NDA), upon written request.
		AAC-02.2		Do you conduct network penetration tests of your cloud service infrastructure regularly as prescribed by industry best practices and guidance?	Yes			Quarterly tests are conducted by third party organizations
		AAC-02.3		Do you conduct application penetration tests of your cloud infrastructure regularly as prescribed by industry best practices and guidance?	Yes			
		AAC-02.4		Do you conduct internal audits regularly as prescribed by industry best practices and guidance?	Yes			
		AAC-02.5		Do you conduct external audits regularly as prescribed by industry best practices and guidance?	Yes			
		AAC-02.6		Are the results of the penetration tests available to tenants at their request?	Yes			Penetration testing summary and response are available upon request and under NDA
		AAC-02.7		Are the results of internal and external audits available to tenants at their request?	Yes			Results of external audits can be shared. Internal (white box) audits can be shared during an onsite visit.
		AAC-02.8		Do you have an internal audit program that allows for cross-functional audit of assessments?	Yes			
Audit Assurance & Compliance *Information System*	AAC-03	AAC-03.1	**Organizations shall create and maintain a control framework which captures standards, regulatory, legal, and statutory requirements relevant for their business needs. The control framework shall be**	Do you have the ability to logically segment or encrypt customer data such that data may be produced for a single tenant only, without inadvertently accessing another tenant's data?	Yes			
		AAC-03.2		Do you have capability to recover data for a specific customer in the case of a failure or data loss?	Yes			

Regulatory Mapping		AAC-03.3	**reviewed at least annually to ensure changes that could affect the business processes are reflected.**	Do you have the capability to restrict the storage of customer data to specific countries or geographic locations?	Yes			This capability is available upon customer request and under special terms.
		AAC-03.4		Do you have a program in place that includes the ability to monitor changes to the regulatory requirements in relevant jurisdictions, adjust your security program for changes to legal requirements, and ensure compliance with relevant regulatory requirements?	Yes			
Business Continuity Management & Operational Resilience *Business Continuity Planning*	BCR-01	BCR-01.1	**A consistent unified framework for business continuity planning and plan development shall be established, documented and adopted to ensure all business continuity plans are consistent in addressing priorities for testing, maintenance, and information security requirements. Requirements for business continuity plans include the following [...]**	Do you provide tenants with geographically resilient hosting options?	Yes			
		BCR-01.2		Do you provide tenants with infrastructure service failover capability to other providers?	Yes			This capability is available upon customer request and under special terms.
Business Continuity Management & Operational Resilience *Business Continuity Testing*	BCR-02	BCR-02.1	**Business continuity and security incident response plans shall be subject to testing at planned intervals or upon significant organizational or environmental changes. Incident response plans shall involve impacted customers (tenant) and other business relationships that represent critical intra-supply chain business process dependencies.**	Are business continuity plans subject to test at planned intervals or upon significant organizational or environmental changes to ensure continuing effectiveness?	Yes			
Business Continuity Management & Operational Resilience *Power / Telecommunications*	BCR-03	BCR-03.1	**Datacenter utilities services and environmental conditions (e.g., water, power, temperature and humidity controls, telecommunications, and internet connectivity) shall be secured, monitored, maintained, and tested for continual effectiveness at planned intervals to ensure protection from unauthorized interception or damage, and designed with automated fail-over or other redundancies in the event of planned or unplanned disruptions.**	Do you provide tenants with documentation showing the transport route of their data between your systems?	Yes			Available upon request and under NDA
		BCR-03.2		Can tenants define how their data is transported and through which legal jurisdictions?		No		Routing configuration is currently not supported. Specific customizations can be done for private cloud deployments
Business Continuity Management & Operational Resilience Documentation	BCR-04	BCR-04.1	**Information system documentation (e.g., administrator and user guides, and architecture diagrams) shall be made available to authorized personnel to ensure the following:** **• Configuring, installing, and operating the information system** **• Effectively using the system's security features**	Are information system documents (e.g., administrator and user guides, architecture diagrams, etc.) made available to authorized personnel to ensure configuration, installation and operation of the information system?	Yes			

Business Continuity Management & Operational Resilience *Environmental Risks*	BCR-05	BCR-05.1	**Physical protection against damage from natural causes and disasters, as well as deliberate attacks, including fire, flood, atmospheric electrical discharge, solar induced geomagnetic storm, wind, earthquake, tsunami, explosion, nuclear accident, volcanic activity, biological hazard, civil unrest, mudslide, tectonic activity, and other forms of natural or man-made disaster shall be anticipated, designed, and have countermeasures applied.**	Is physical protection against damage (e.g., natural causes, natural disasters, deliberate attacks) anticipated and designed with countermeasures applied?	Yes			
Business Continuity Management & Operational Resilience *Equipment Location*	BCR-06	BCR-06.1	**To reduce the risks from environmental threats, hazards, and opportunities for unauthorized access, equipment shall be kept away from locations subject to high probability environmental risks and supplemented by redundant equipment located at a reasonable distance.**	Are any of your data centers located in places that have a high probability/occurrence of high-impact environmental risks (floods, tornadoes, earthquakes, hurricanes, etc.)?		No		
Business Continuity Management & Operational Resilience *Equipment Maintenance*	BCR-07	BCR-07.1	**Policies and procedures shall be established, and supporting business processes and technical measures implemented, for equipment maintenance ensuring continuity and availability of operations and support personnel.**	If using virtual infrastructure, does your cloud solution include independent hardware restore and recovery capabilities?	Yes			The Adallom infrastructure does not depend on a specific provider
		BCR-07.2		If using virtual infrastructure, do you provide tenants with a capability to restore a Virtual Machine to a previous state in time?			N/A	Adallom is not an IaaS provider
		BCR-07.3		If using virtual infrastructure, do you allow virtual machine images to be downloaded and ported to a new cloud provider?			N/A	Adallom is not an IaaS provider
		BCR-07.4		If using virtual infrastructure, are machine images made available to the customer in a way that would allow the customer to replicate those images in their own off-site storage location?	Yes			Relevant only for private cloud deployments
		BCR-07.5		Does your cloud solution include software/provider independent restore and recovery capabilities?	Yes			
Business Continuity Management & Operational Resilience *Equipment Power Failures*	BCR-08	BCR-08.1	**Protection measures shall be put into place to react to natural and man-made threats based upon a geographically-specific Business Impact Assessment**	Are security mechanisms and redundancies implemented to protect equipment from utility service outages (e.g., power failures, network disruptions, etc.)?	Yes			
Business Continuity Management & Operational Resilience	BCR-09	BCR-09.1	**There shall be a defined and documented method for determining the impact of any disruption to the organization (cloud provider, cloud consumer) that must incorporate the following:** **[…]**	Do you provide tenants with ongoing visibility and reporting of your operational Service Level Agreement (SLA) performance?	Yes			
		BCR-09.2		Do you make standards-based information security metrics (CSA, CAMM, etc.) available to your tenants?	Yes			

Impact Analysis		BCR-09.3		Do you provide customers with ongoing visibility and reporting of your SLA performance?	Yes			
Business Continuity Management & Operational Resilience *Policy*	BCR-10	BCR-10.1	**Policies and procedures shall be established, and supporting business processes and technical measures implemented, for appropriate IT governance and service management to ensure appropriate planning, delivery and support of the organization's IT capabilities supporting business functions, workforce, and/or customers based on industry acceptable standards (i.e., ITIL v4 and COBIT 5). Additionally, policies and procedures shall include defined roles and responsibilities supported by regular workforce training.**	Are policies and procedures established and made available for all personnel to adequately support services operations' roles?	Yes			
Business Continuity Management & Operational Resilience *Retention Policy*	BCR-11	BCR-11.1	**Policies and procedures shall be established, and supporting business processes and technical measures implemented, for defining and adhering to the retention period of any critical asset as per established policies and procedures, as well as applicable legal, statutory, or regulatory compliance obligations. Backup and recovery measures shall be incorporated as part of business continuity planning and tested accordingly for effectiveness.**	Do you have technical control capabilities to enforce tenant data retention policies?	Yes			
		BCR-11.2		Do you have a documented procedure for responding to requests for tenant data from governments or third parties?	Yes			
		BCR-11.4		Have you implemented backup or redundancy mechanisms to ensure compliance with regulatory, statutory, contractual or business requirements?	Yes			
		BCR-11.5		Do you test your backup or redundancy mechanisms at least annually?	Yes			
Change Control & Configuration Management *New Development / Acquisition*	CCC-01	CCC-01.1	**Policies and procedures shall be established, and supporting business processes and technical measures implemented, to ensure the development and/or acquisition of new data, physical or virtual applications, infrastructure network and systems components, […]**	Are policies and procedures established for management authorization for development or acquisition of new applications, systems, databases, infrastructure, services, operations and facilities?	Yes			
		CCC-01.2		Is documentation available that describes the installation, configuration and use of products/services/features?	Yes			
Change Control & Configuration Management *Outsourced Development*	CCC-02	CCC-02.1	**External business partners shall adhere to the same policies and procedures for change management, release, and testing as internal developers within the organization (e.g. ITIL service management processes).**	Do you have controls in place to ensure that standards of quality are being met for all software development?	Yes			
		CCC-02.2		Do you have controls in place to detect source code security defects for any outsourced software development activities?			N/A	Core software development is not outsourced.
Change Control & Configuration *Management Quality Testing*	CCC-03	CCC-03.1	**Organization shall follow a defined quality change control and testing process (e.g. ITIL Service Management) with established baselines, testing and release standards which focus on system availability, confidentiality and integrity of systems and services**	Do you provide your tenants with documentation that describes your quality assurance process?	Yes			Can be provided upon request and under NDA
		CCC-03.2		Is documentation describing known issues with certain products/services available?	Yes			
		CCC-03.3		Are there policies and procedures in place to triage and remedy reported bugs and security vulnerabilities for product and service offerings?	Yes			
		CCC-03.4		Are mechanisms in place to ensure that all debugging and test code elements are removed from released software versions?	Yes			

Change Control & Configuration Management *Unauthorized Software Installations*	CCC-04	CCC-04.1	**Policies and procedures shall be established, and supporting business processes and technical measures implemented, to restrict the installation of unauthorized software on organizationally-owned or managed user end-point devices (e.g., issued workstations, laptops, and mobile devices) and IT infrastructure network and systems components.**	Do you have controls in place to restrict and monitor the installation of unauthorized software onto your systems?	Yes			
Change Control & Configuration Management *Production Changes*	CCC-05	CCC-05.1	**Policies and procedures shall be established for managing the risks associated with applying changes to business-critical or customer (tenant) impacting (physical and virtual) application and system-system interface (API) designs and configurations, […]**	Do you provide tenants with documentation that describes your production change management procedures and their roles/rights/responsibilities within it?	Yes			Can be provided upon request and under NDA
Data Security & Information Lifecycle Management *Classification*	DSI-01	DSI-01.1	**Data and objects containing data shall be assigned a classification by the data owner based on data type, value, sensitivity, and criticality to the organization.**	Do you provide a capability to identify virtual machines via policy tags/metadata (e.g., tags can be used to limit guest operating systems from booting/instantiating/transporting data in the wrong country)?	Yes			
		DSI-01.2		Do you provide a capability to identify hardware via policy tags/metadata/hardware tags (e.g., TXT/TPM, VN-Tag, etc.)?	Yes			
		DSI-01.3		Do you have a capability to use system geographic location as an authentication factor?	Yes			
		DSI-01.4		Can you provide the physical location/geography of storage of a tenant's data upon request?	Yes			
		DSI-01.5		Can you provide the physical location/geography of storage of a tenant's data in advance?	Yes			
		DSI-01.6		Do you follow a structured data-labelling standard (e.g., ISO 15489, Oasis XML Catalog Specification, CSA data type guidance)?	Yes			
		DSI-01.7		Do you allow tenants to define acceptable geographical locations for data routing or resource instantiation?		No		Not supported for SaaS offering. Adallom can accommodate this request in a private cloud deployment
Data Security & Information Lifecycle Management *Data Inventory / Flows*	DSI-02	DSI-02.1	**Policies and procedures shall be established to inventory, document, and maintain data flows for data that is resident (permanently or temporarily) within the service's applications and infrastructure network and systems. In particular, providers shall ensure that data that is subject to geographic residency requirements not be migrated beyond its defined bounds.**	Do you inventory, document, and maintain data flows for data that is resident (permanent or temporary) within the services' applications and infrastructure network and systems?	Yes			
		DSI-02.2		Can you ensure that data does not migrate beyond a defined geographical residency?		No		Not supported for SaaS offering. Adallom can accommodate this request in a private cloud deployment
Data Security & Information Lifecycle Management *eCommerce*	DSI-03	DSI-03.1	**Data related to electronic commerce (e-commerce) that traverses public networks shall be appropriately classified and protected from fraudulent activity, unauthorized disclosure, or modification in such a manner to prevent contract dispute and compromise**	Do you provide open encryption methodologies (3.4ES, AES, etc.) to tenants in order for them to protect their data if it is required to move through public networks (e.g., the Internet)?	Yes			Adallom uses industry standard SSL for data transmitted across public networks.
		DSI-03.2		Do you utilize open encryption methodologies any time your infrastructure components need to communicate with each other via public networks (e.g., Internet-based replication of data from one environment to another)?	Yes			

Transactions			**of data.**					
Data Security & Information Lifecycle Management *Handling / Labelling / Security Policy*	DSI-04	DSI-04.1	**Policies and procedures shall be established for labelling, handling, and the security of data and objects which contain data. Mechanisms for label inheritance shall be implemented for objects that act as aggregate containers for data.**	Are policies and procedures established for labelling, handling and the security of data and objects that contain data?	Yes			
		DSI-04.2		Are mechanisms for label inheritance implemented for objects that act as aggregate containers for data?	Yes			
Data Security & Information Lifecycle Management *Nonproduction Data*	DSI-05	DSI-05.1	**Production data shall not be replicated or used in non-production environments.**	Do you have procedures in place to ensure production data shall not be replicated or used in non-production environments?	Yes			Basic inheritance through folder and sub folder permissions
Data Security & Information Lifecycle Management *Ownership / Stewardship*	DSI-06	DSI-06.1	**All data shall be designated with stewardship, with assigned responsibilities defined, documented, and communicated.**	Are the responsibilities regarding data stewardship defined, assigned, documented and communicated?	Yes			
Data Security & Information Lifecycle Management *Secure Disposal*	DSI-07	DSI-07.1	**Any use of customer data in non-production environments requires explicit, documented approval from all customers whose data is affected, and must comply with all legal and regulatory requirements for scrubbing of sensitive data elements.**	Do you support secure deletion (e.g., degaussing/cryptographic wiping) of archived and backed-up data as determined by the tenant?	Yes			
		DSI-07.2		Can you provide a published procedure for exiting the service arrangement, including assurance to sanitize all computing resources of tenant data once a customer has exited your environment or has vacated a resource?	Yes			
Datacenter Security *Asset Management*	DCS-01	DCS-01.1	**Assets must be classified in terms of business criticality, service-level expectations, and operational continuity requirements. A complete inventory of business-critical assets located at all sites and/or geographical locations and their usage over time shall be maintained and updated regularly, and assigned ownership y defined roles and responsibilities.**	Do you maintain a complete inventory of all of your critical assets that includes ownership of the asset?	Yes			
		DCS-01.2		Do you maintain a complete inventory of all of your critical supplier relationships?	Yes			

Datacenter Security *Controlled Access Points*	DCS-02	DCS-02.1	**Physical security perimeters (e.g., fences, walls, barriers, guards, gates, electronic surveillance, physical authentication mechanisms, reception desks, and security patrols) shall be implemented to safeguard sensitive data and information systems.**	Are physical security perimeters (e.g., fences, walls, barriers, guards, gates, electronic surveillance, physical authentication mechanisms, reception desks and security patrols) implemented?	Yes			
Datacenter Security *Equipment Identification*	DCS-03	DCS-03.1	**Automated equipment identification shall be used as a method of connection authentication. Location-aware technologies may be used to validate connection authentication integrity based on known equipment location.**	Is automated equipment identification used as a method to validate connection authentication integrity based on known equipment location?		No		
Datacenter Security *Offsite Authorization*	DCS-04	DCS-04.1	**Authorization must be obtained prior to relocation or transfer of hardware, software, or data to an offsite premises.**	Do you provide tenants with documentation that describes scenarios in which data may be moved from one physical location to another? (e.g., offsite backups, business continuity failovers, replication)	Yes			Can be provided upon request and under NDA
Datacenter Security *Offsite equipment*	DCS-05	DCS-05.1	**Policies and procedures shall be established for the secure disposal of equipment (by asset type) used outside the organization's premise. This shall include a wiping solution or destruction process that renders recovery of information impossible. The erasure shall consist of a full write of the drive to ensure that the erased drive is released to inventory for reuse and deployment or securely stored until it can be destroyed.**	Can you provide tenants with evidence documenting your policies and procedures governing asset management and repurposing of equipment?	Yes			
Datacenter Security *Policy*	DCS-06	DCS-06.1	**Policies and procedures shall be established, and supporting business processes implemented, for maintaining a safe and secure working environment in offices, rooms, facilities, and secure areas.**	Can you provide evidence that policies, standards and procedures have been established for maintaining a safe and secure working environment in offices, rooms, facilities and secure areas?	Yes			
		DCS-06.2		Can you provide evidence that your personnel and involved third parties have been trained regarding your documented policies, standards and procedures?	Yes			
Datacenter Security *Secure Area Authorization*	DCS-07	DCS-07.1	**Ingress and egress to secure areas shall be constrained and monitored by physical access control mechanisms to ensure that only authorized personnel are allowed access.**	Do you allow tenants to specify which of your geographic locations their data is allowed to move into/out of (to address legal jurisdictional considerations based on where data is stored vs. accessed)?		No		Not supported for SaaS offering. Adallom can accommodate this request in a private cloud deployment
Datacenter Security *Unauthorized Persons Entry*	DCS-08	DCS-08.1	**Ingress and egress points such as service areas and other points where unauthorized personnel may enter the premises shall be monitored, controlled and, if possible, isolated from data storage and processing facilities to prevent unauthorized data corruption, compromise, and loss.**	Are ingress and egress points, such as service areas and other points where unauthorized personnel may enter the premises, monitored, controlled and isolated from data storage and process?	Yes			

Datacenter Security *User Access*	DCS-09	DCS-09.1	**Physical access to information assets and functions by users and support personnel shall be restricted.**	Do you restrict physical access to information assets and functions by users and support personnel?	Yes			
Encryption & Key Management *Entitlement*	EKM-01	EKM-01.1	**Keys must have identifiable owners (binding keys to identities) and there shall be key management policies.**	Do you have key management policies binding keys to identifiable owners?	Yes			
Encryption & Key Management *Key Generation*	EKM-02	EKM-02.1	**Policies and procedures shall be established for the management of cryptographic keys in the service's cryptosystem (e.g., lifecycle management from key generation to revocation and replacement, public key infrastructure, cryptographic protocol design and algorithms used, access controls in place for secure key generation, and exchange and storage including segregation of keys used for encrypted data or sessions). Upon request, provider shall inform the customer (tenant) of changes within the cryptosystem, especially if the customer (tenant) data is used as part of the service, and/or the customer (tenant) has some shared responsibility over implementation of the control.**	Do you have a capability to allow creation of unique encryption keys per tenant?		No		
		EKM-02.2		Do you have a capability to manage encryption keys on behalf of tenants?	Yes			
		EKM-02.3		Do you maintain key management procedures?	Yes			
		EKM-02.4		Do you have documented ownership for each stage of the lifecycle of encryption keys?	Yes			
		EKM-02.5		Do you utilize any third party/open source/proprietary frameworks to manage encryption keys?	Yes			
Encryption & Key Management *Encryption*	EKM-03	EKM-03.1	**Policies and procedures shall be established, and supporting business processes and technical measures implemented, for the use of encryption protocols for protection of sensitive data in storage (e.g., file servers, databases, and end-user workstations) and data in transmission (e.g., system interfaces, over public networks, and electronic messaging) as per applicable legal, statutory, and regulatory compliance obligations.**	Do you encrypt tenant data at rest (on disk/storage) within your environment?	Yes			Applicable for specific data sets
		EKM-03.2		Do you leverage encryption to protect data and virtual machine images during transport across and between networks and hypervisor instances?	Yes			
		EKM-03.3		Do you support tenant-generated encryption keys or permit tenants to encrypt data to an identity without access to a public key certificate (e.g. identity-based encryption)?	Yes			Can be implemented through integration with a 3rd party encryption service
		EKM-03.4		Do you have documentation establishing and defining your encryption management policies, procedures and guidelines?	Yes			
Encryption & Key Management *Storage and Access*	EKM-04	EKM-04.1	**Platform and data appropriate encryption (e.g., AES-256) in open/validated formats and standard algorithms shall be required. Keys shall not be stored in the cloud (i.e. at the cloud provider in question), but maintained by the cloud consumer or trusted key**	Do you have platform and data appropriate encryption that uses open/validated formats and standard algorithms?	Yes			
		EKM-04.2		Are your encryption keys maintained by the cloud consumer or a trusted key management provider?	Yes			Applicable for customers who deployed the encryption integration

		EKM-04.3	**management provider. Key management and key usage shall be separated duties.**	Do you store encryption keys in the cloud?	Yes			
		EKM-04.4		Do you have separate key management and key usage duties?	Yes			
Governance and Risk Management *Baseline Requirements*	GRM-01	GRM-01.1	**Baseline security requirements shall be established for developed or acquired, organizationally-owned or managed, physical or virtual, applications and infrastructure system and network components that comply with applicable legal, statutory and regulatory compliance obligations. Deviations from standard baseline configurations must be authorized following change management policies and procedures prior to deployment, provisioning, or use. Compliance with security baseline requirements must be reassessed at least annually unless an alternate frequency has been established and established and authorized based on business need.**	Do you have documented information security baselines for every component of your infrastructure (e.g., hypervisors, operating systems, routers, DNS servers, etc.)?	Yes			
		GRM-01.2		Do you have a capability to continuously monitor and report the compliance of your infrastructure against your information security baselines?	Yes			
		GRM-01.3		Do you allow your clients to provide their own trusted virtual machine image to ensure conformance to their own internal standards?	Yes			Applicable only for private cloud deployment
Governance and Risk Management *Risk Assessments*	GRM-02	GRM-02.1	**Risk assessments associated with data governance requirements shall be conducted at planned intervals and shall consider the following:** **• Awareness of where sensitive data is stored and transmitted across applications, databases, servers, and network infrastructure** **• Compliance with defined retention periods and end-of-life disposal requirements** **• Data classification and protection from unauthorized use, access, loss, destruction, and falsification**	Do you provide security control health data in order to allow tenants to implement industry standard Continuous Monitoring (which allows continual tenant validation of your physical and logical control status)?		No		Available through SOC2 controls documents. This information is not yet available through APIs.
		GRM-02.2		Do you conduct risk assessments associated with data governance requirements at least once a year?	Yes			
Governance and Risk Management *Management Oversight*	GRM-03	GRM-03.1	**Managers are responsible for maintaining awareness of, and complying with, security policies, procedures and standards that are relevant to their area of responsibility.**	Are your technical, business, and executive managers responsible for maintaining awareness of and compliance with security policies, procedures, and standards for both themselves and their employees as they pertain to the manager and employees' area of responsibility?	Yes			
Governance and Risk Management *Management Program*	GRM-04	GRM-04.1	**An Information Security Management Program (ISMP) shall be developed, documented, approved, and implemented that includes administrative, technical, and physical safeguards to protect assets and data from loss, misuse, unauthorized access,**	Do you provide tenants with documentation describing your Information Security Management Program (ISMP)?	Yes			
		GRM-		Do you review your Information Security Management Program (ISMP) least once a year?	Yes			

		04.2	**disclosure, alteration, and destruction. The security program shall include, but not be limited to, the following areas insofar as they relate to the characteristics of the business: […]**					
Governance and Risk Management *Management Support / Involvement*	GRM-05	GRM-05.1	**Executive and line management shall take formal action to support information security through clearly-documented direction and commitment, and shall ensure the action has been assigned.**	Do you ensure your providers adhere to your information security and privacy policies?	Yes			Adallom contracts only with services that adhere to standards set by Adallom's policies where applicable.
Governance and Risk Management *Policy*	GRM-06	GRM-06.1	**Information security policies and procedures shall be established and made readily available for review by all impacted personnel and external business relationships. Information security policies must be authorized by the organization's business leadership (or other accountable business role or function) and supported by a strategic business plan and an information security management program inclusive of defined information security roles and responsibilities for business leadership.**	Do your information security and privacy policies align with industry standards (ISO-27001, ISO-22307, CoBIT, etc.)?	Yes			Annual SOC2 type 2 audit is performed
		GRM-06.2		Do you have agreements to ensure your providers adhere to your information security and privacy policies?	Yes			
		GRM-06.3		Can you provide evidence of due diligence mapping of your controls, architecture and processes to regulations and/or standards?	Yes			
		GRM-06.4		Do you disclose which controls, standards, certifications and/or regulations you comply with?	Yes			
Governance and Risk Management *Policy Enforcement*	GRM-07	GRM-07.1	**A formal disciplinary or sanction policy shall be established for employees who have violated security policies and procedures. Employees shall be made aware of what action might be taken in the event of a violation, and disciplinary measures must be stated in the policies and procedures.**	Is a formal disciplinary or sanction policy established for employees who have violated security policies and procedures?	Yes			
		GRM-07.2		Are employees made aware of what actions could be taken in the event of a violation via their policies and procedures?	Yes			
Governance and Risk Management *Business / Policy Change Impacts*	GRM-08	GRM-08.1	**Risk assessment results shall include updates to security policies, procedures, standards, and controls to ensure that they remain relevant and effective.**	Do risk assessment results include updates to security policies, procedures, standards and controls to ensure they remain relevant and effective?	Yes			
Governance and Risk Management *Policy Reviews*	GRM-09	GRM-09.1	**The organization's business leadership (or other accountable business role or function) shall review the information security policy at planned intervals or as a result of changes to the organization to ensure its continuing alignment with the security strategy, effectiveness, accuracy, relevance, and applicability to legal, statutory, or regulatory compliance obligations.**	Do you notify your tenants when you make material changes to your information security and/or privacy policies?	Yes			
		GRM-09.2		Do you perform, at minimum, annual reviews to your privacy and security policies?	Yes			

Governance and Risk Management *Assessments*	GRM-10	GRM-10.1	**Aligned with the enterprise-wide framework, formal risk assessments shall be performed at least annually or at planned intervals, (and in conjunction with any changes to information systems) to determine the likelihood and impact of all identified risks using qualitative and quantitative methods. The likelihood and impact associated with inherent and residual risk shall be determined independently, considering all risk categories (e.g., audit results, threat and vulnerability analysis, and regulatory compliance).**	Are formal risk assessments aligned with the enterprise-wide framework and performed at least annually, or at planned intervals, determining the likelihood and impact of all identified risks, using qualitative and quantitative methods?	Yes			
		GRM-10.2		Is the likelihood and impact associated with inherent and residual risk determined independently, considering all risk categories (e.g., audit results, threat and vulnerability analysis, and regulatory compliance)?	Yes			
Governance and Risk Management *Program*	GRM-11	GRM-11.1	**Organizations shall develop and maintain an enterprise risk management framework to mitigate risk to an acceptable level.**	Do you have a documented, organization-wide program in place to manage risk?	Yes			
		GRM-11.2		Do you make available documentation of your organization-wide risk management program?	Yes			Available upon request and under NDA
Human Resources *Asset Returns*	HRS-01	HRS-01.1	**Upon termination of workforce personnel and/or expiration of external business relationships, all organizationally-owned assets shall be returned within an established period.**	Are systems in place to monitor for privacy breaches and notify tenants expeditiously if a privacy event may have impacted their data?	Yes			
		HRS-01.2		Is your Privacy Policy aligned with industry standards?	Yes			
Human Resources *Background Screening*	HRS-02	HRS-02.1	**Pursuant to local laws, regulations, ethics, and contractual constraints, all employment candidates, contractors, and third parties shall be subject to background verification proportional to the data classification to be accessed, the business requirements, and acceptable risk.**	Pursuant to local laws, regulations, ethics and contractual constraints, are all employment candidates, contractors and involved third parties subject to background verification?	Yes			
Human Resources *Employment Agreements*	HRS-03	HRS-03.1	**Employment agreements shall incorporate provisions and/or terms for adherence to established information governance and security policies and must be signed by newly hired or on-boarded workforce personnel (e.g., full or part-time employee or contingent staff) prior to granting workforce personnel user access to corporate facilities, resources, and assets.**	Do you specifically train your employees regarding their specific role and the information security controls they must fulfil?	Yes			
		HRS-03.2		Do you document employee acknowledgment of training they have completed?	Yes			
		HRS-03.3		Are all personnel required to sign NDA or Confidentiality Agreements as a condition of employment to protect customer/tenant information?	Yes			
		HRS-03.4		Is successful and timed completion of the training program considered a prerequisite for acquiring and maintaining access to sensitive systems?	Yes			
		HRS-03.5		Are personnel trained and provided with awareness programs at least once a year?	Yes			
Human Resources *Employment Termination*	HRS-04	HRS-04.1	**Roles and responsibilities for performing employment termination or change in employment procedures shall be assigned, documented, and communicated.**	Are documented policies, procedures and guidelines in place to govern change in employment and/or termination?	Yes			
		HRS-04.2		Do the above procedures and guidelines account for timely revocation of access and return of assets?	Yes			

Human Resources *Portable / Mobile Devices*	HRS-05	HRS-05.1	**Policies and procedures shall be established, and supporting business processes and technical measures implemented, to manage business risks associated with permitting mobile device access to corporate resources and may require the implementation of higher assurance compensating controls and acceptable-use policies and procedures (e.g., mandated security training, stronger identity, entitlement and access controls, and device monitoring).**	Are policies and procedures established and measures implemented to strictly limit access to your sensitive data and tenant data from portable and mobile devices (e.g. laptops, cell phones and personal digital assistants (PDAs)), which are generally higher-risk than non-portable devices (e.g., desktop computers at the provider organization's facilities)?	Yes			
Human Resources *Nondisclosure Agreements*	HRS-06	HRS-06.1	**Requirements for non-disclosure or confidentiality agreements reflecting the organization's needs for the protection of data and operational details shall be identified, documented, and reviewed at planned intervals.**	Are requirements for non-disclosure or confidentiality agreements reflecting the organization's needs for the protection of data and operational details identified, documented and reviewed at planned intervals?	Yes			Requirements for NDAs and confidentiality agreements are documented. There is no planned interval for review.
Human Resources *Roles / Responsibilities*	HRS-07	HRS-07.1	**Roles and responsibilities of contractors, employees, and third-party users shall be documented as they relate to information assets and security.**	Do you provide tenants with a role definition document clarifying your administrative responsibilities versus those of the tenant?	Yes			Available upon request and under NDA
Human Resources *Acceptable Use*	HRS-08	HRS-08.1	**Policies and procedures shall be established, and supporting business processes and technical measures implemented, for defining allowances and conditions for permitting usage of organizationally-owned or managed user end-point devices (e.g., issued workstations, laptops, and mobile devices) and IT infrastructure network and systems components. Additionally, defining allowances and conditions to permit usage of personal mobile devices and associated applications with access to corporate resources (i.e., BYOD) shall be considered and incorporated as appropriate.**	Do you provide documentation regarding how you may or access tenant data and metadata?	Yes			
		HRS-08.2		Do you collect or create metadata about tenant data usage through inspection technologies (search engines, etc.)?	Yes			
		HRS-08.3		Do you allow tenants to opt out of having their data/metadata accessed via inspection technologies?	Yes			
Human Resources *Training / Awareness*	HRS-09	HRS-09.1	**A security awareness training program shall be established for all contractors, third-party users, and employees of the organization and mandated when appropriate. All individuals with access to organizational data shall receive appropriate awareness training and regular updates in organizational procedures, processes, and policies relating to their professional function relative to the**	Do you provide a formal, role-based, security awareness training program for cloud-related access and data management issues (e.g., multi-tenancy, nationality, cloud delivery model segregation of duties implications and conflicts of interest) for all persons with access to tenant data?	Yes			
		HRS-09.2		Are administrators and data stewards properly educated on their legal responsibilities with regard to security and data integrity?	Yes			

			organization.					
Human Resources *User Responsibility*	HRS-10	HRS-10.1	**All personnel shall be made aware of their roles and responsibilities for:** **• Maintaining awareness and compliance with established policies and procedures and applicable legal, statutory, or regulatory compliance obligations.** **• Maintaining a safe and secure working environment**	Are users made aware of their responsibilities for maintaining awareness and compliance with published security policies, procedures, standards and applicable regulatory requirements?	Yes			
		HRS-10.2		Are users made aware of their responsibilities for maintaining a safe and secure working environment?	Yes			
		HRS-10.3		Are users made aware of their responsibilities for leaving unattended equipment in a secure manner?	Yes			
Human Resources *Workspace*	HRS-11	HRS-11.1	**Policies and procedures shall be established to require that unattended workspaces do not have openly visible (e.g., on a desktop) sensitive documents and user computing sessions had been disabled after an established period of inactivity.**	Do your data management policies and procedures address tenant and service level conflicts of interests?	Yes			Adallom's policies and procedures address service SLAs.
		HRS-11.2		Do your data management policies and procedures include a tamper audit or software integrity function for unauthorized access to tenant data?	Yes			
		HRS-11.3		Does the virtual machine management infrastructure include a tamper audit or software integrity function to detect changes to the build/configuration of the virtual machine?	Yes			Adallom uses its own service which provides detection for unauthorized access to virtual infrastructure management
Identity & Access Management *Audit Tools Access*	IAM-01	IAM-01.1	**Access to, and use of, audit tools that interact with the organization's information systems shall be appropriately segmented and restricted to prevent compromise and misuse of log data.**	Do you restrict, log and monitor access to your information security management systems? (E.g., hypervisors, firewalls, vulnerability scanners, network sniffers, APIs, etc.)	Yes			
		IAM-01.2		Do you monitor and log privileged access (administrator level) to information security management systems?	Yes			
Identity & Access Management *User Access Policy*	IAM-02	IAM-02.1	**User access policies and procedures shall be established, and supporting business processes and technical measures implemented, for ensuring appropriate identity, entitlement, and access management for all internal corporate and customer (tenant) users with access to data and organizationally-owned or managed (physical and virtual) application interfaces and infrastructure network and systems components. […]**	Do you have controls in place ensuring timely removal of systems access that is no longer required for business purposes?	Yes			
		IAM-02.2		Do you provide metrics to track the speed with which you are able to remove systems access that is no longer required for business purposes?		No		
Identity & Access	IAM-03	IAM-03.1	**User access to diagnostic and configuration ports shall be restricted to authorized individuals and**	Do you use dedicated secure networks to provide management access to your cloud service infrastructure?	Yes			

Management *Diagnostic / Configuration Ports Access*			**applications.**					
Identity & Access Management *Policies and Procedures*	IAM-04	IAM-04.1	**Policies and procedures shall be established to store and manage identity information about every person who accesses IT infrastructure and to determine their level of access. Policies shall also be developed to control access to network resources based on user identity.**	Do you manage and store the identity of all personnel who have access to the IT infrastructure, including their level of access?	Yes			
		IAM-04.2		Do you manage and store the user identity of all personnel who have network access, including their level of access?	Yes			
Identity & Access Management *Segregation of Duties*	IAM-05	IAM-05.1	**User access policies and procedures shall be established, and supporting business processes and technical measures implemented, for restricting user access as per defined segregation of duties to address business risks associated with a user-role conflict of interest.**	Do you provide tenants with documentation on how you maintain segregation of duties within your cloud service offering?	Yes			
Identity & Access Management *Source Code Access Restriction*	IAM-06	IAM-06.1	**Access to the organization's own developed applications, program, or object source code, or any other form of intellectual property (IP), and use of proprietary software shall be appropriately restricted following the rule of least privilege based on job function as per established user access policies and procedures.**	Are controls in place to prevent unauthorized access to your application, program or object source code, and assure it is restricted to authorized personnel only?	Yes			
		IAM-06.2		Are controls in place to prevent unauthorized access to tenant application, program or object source code, and assure it is restricted to authorized personnel only?	Yes			
Identity & Access Management *Third Party Access*	IAM-07	IAM-07.1	**The identification, assessment, and prioritization of risks posed by business processes requiring third-party access to the organization's information systems and data shall be followed by coordinated application of resources to minimize, monitor, and measure likelihood and impact of unauthorized or inappropriate access. Compensating controls derived from the risk analysis shall be implemented prior to provisioning access.**	Do you provide multi-failure disaster recovery capability?	Yes			
		IAM-07.2		Do you monitor service continuity with upstream providers in the event of provider failure?	Yes			
		IAM-07.3		Do you have more than one provider for each service you depend on?	Yes			
		IAM-07.4		Do you provide access to operational redundancy and continuity summaries, including the services you depend on?	Yes			
		IAM-07.5		Do you provide the tenant the ability to declare a disaster?		No		
		IAM-07.6		Do you provided a tenant-triggered failover option?		No		
		IAM-07.7		Do you share your business continuity and redundancy plans with your tenants?	Yes			Available upon request and under NDA
Identity & Access Management *User Access Restriction / Authorization*	IAM-08	IAM-08.1	**Policies and procedures are established for permissible storage and access of identities used for authentication to ensure identities are only accessible based on rules of least privilege and replication limitation only to users explicitly defined as business necessary.**	Do you document how you grant and approve access to tenant data?	Yes			
		IAM-08.2		Do you have a method of aligning provider and tenant data classification methodologies for access control purposes?	Yes			All customer data is classified as "Customer Data" which is the most sensitive category. Access to customer data is monitored and approved by the customer

Identity & Access Management *User Access Authorization*	IAM-09	IAM-09.1	**Provisioning user access (e.g., employees, contractors, customers (tenants), business partners and/or supplier relationships) to data and organizationally-owned or managed (physical and virtual) applications, infrastructure systems, and network components shall be authorized by the organization's management prior to access being granted and appropriately restricted as per established policies and procedures. Upon request, provider shall inform customer (tenant) of this user access, especially if customer (tenant) data is used as part of the service and/or customer (tenant) has some shared responsibility over implementation of control.**	Does your management provision the authorization and restrictions for user access (e.g. employees, contractors, customers (tenants), business partners and/or suppliers) prior to their access to data and any owned or managed (physical and virtual) applications, infrastructure systems and network components?	Yes			
		IAM-09.2		Do your provide upon request user access (e.g. employees, contractors, customers (tenants), business partners and/or suppliers) to data and any owned or managed (physical and virtual) applications, infrastructure systems and network components?	Yes			
Identity & Access Management *User Access Reviews*	IAM-10	IAM-10.1	**User access shall be authorized and revalidated for entitlement appropriateness, at planned intervals, by the organization's business leadership or other accountable business role or function supported by evidence to demonstrate the organization is adhering to the rule of least privilege based on job function. For identified access violations, remediation must follow established user access policies and procedures.**	Do you require at least annual certification of entitlements for all system users and administrators (exclusive of users maintained by your tenants)?	Yes			
		IAM-10.2		If users are found to have inappropriate entitlements, are all remediation and certification actions recorded?	yes			
		IAM-10.3		Will you share user entitlement remediation and certification reports with your tenants, if inappropriate access may have been allowed to tenant data?	yes			
Identity & Access Management *User Access Revocation*	IAM-11	IAM-11.1	**Timely de-provisioning (revocation or modification) of user access to data and organizationally-owned or managed (physical and virtual) applications, infrastructure systems, and network components, shall be implemented as per established policies and procedures and based on user's change in status (e.g., termination of employment or other business relationship, job change or transfer). Upon request, provider shall inform customer (tenant) of these changes, especially if customer (tenant) data is used as part the service and/or customer (tenant) has some shared responsibility over implementation of control.**	Is timely deprovisioning, revocation or modification of user access to the organizations systems, information assets and data implemented upon any change in status of employees, contractors, customers, business partners or involved third parties?	Yes			
		IAM-11.2		Is any change in user access status intended to include termination of employment, contract or agreement, change of employment or transfer within the organization?	Yes			
Identity & Access Management *User ID Credentials*	IAM-12	IAM-12.1	**Internal corporate or customer (tenant) user account credentials shall be restricted as per the following, ensuring appropriate identity, entitlement, and access management and in accordance with established policies and procedures:**	Do you support use of, or integration with, existing customer-based Single Sign On (SSO) solutions to your service?	Yes			
		IAM-12.2		Do you use open standards to delegate authentication capabilities to your tenants?	Yes			
		IAM-12.3		Do you support identity federation standards (SAML, SPML, WS-Federation, etc.) as a means of authenticating/authorizing users?	Yes			

		IAM-12.4	• **Identity trust verification and service-to-service application (API) and information processing interoperability (e.g., SSO and Federation)** • **Account credential lifecycle management from instantiation through revocation** • **Account credential and/or identity store minimization or re-use when feasible** • **Adherence to industry acceptable and/or regulatory compliant authentication, authorization, and accounting (AAA) rules (e.g., strong/multi-factor, expireable, non-shared authentication secrets)**	Do you have a Policy Enforcement Point capability (e.g., XACML) to enforce regional legal and policy constraints on user access?	Yes			
		IAM-12.5		Do you have an identity management system (enabling classification of data for a tenant) in place to enable both role-based and context-based entitlement to data?	Yes			
		IAM-12.6		Do you provide tenants with strong (multifactor) authentication options (digital certs, tokens, biometrics, etc.) for user access?	Yes			
		IAM-12.7		Do you allow tenants to use third-party identity assurance services?	Yes			
		IAM-12.8		Do you support password (minimum length, age, history, complexity) and account lockout (lockout threshold, lockout duration) policy enforcement?	Yes			
		IAM-12.9		Do you allow tenants/customers to define password and account lockout policies for their accounts?	Yes			
		IAM-12.10		Do you support the ability to force password changes upon first logon?		No		
		IAM-12.11		Do you have mechanisms in place for unlocking accounts that have been locked out (e.g., self-service via email, defined challenge questions, manual unlock)?	Yes			Service is provided by the Adallom support team
Identity & Access Management *Utility Programs Access*	IAM-13	IAM-13.1	**Utility programs capable of potentially overriding system, object, network, virtual machine, and application controls shall be restricted.**	Are utilities that can significantly manage virtualized partitions (e.g., shutdown, clone, etc.) appropriately restricted and monitored?			N/A	Adallom is not a IaaS provider
		IAM-13.2		Do you have a capability to detect attacks that target the virtual infrastructure directly (e.g., shimming, Blue Pill, Hyper jumping, etc.)?			N/A	Adallom is not a IaaS provider
		IAM-13.3		Are attacks that target the virtual infrastructure prevented with technical controls?			N/A	Adallom is not a IaaS provider
Infrastructure & Virtualization Security *Audit Logging / Intrusion Detection*	IVS-01	IVS-01.1	**Higher levels of assurance are required for protection, retention, and lifecycle management of audit logs, adhering to applicable legal, statutory or regulatory compliance obligations and providing unique user access accountability to detect potentially suspicious network behaviors and/or file integrity anomalies, and to support forensic investigative capabilities in the event of a security breach.**	Are file integrity (host) and network intrusion detection (IDS) tools implemented to help facilitate timely detection, investigation by root cause analysis and response to incidents?	Yes			
		IVS-01.2		Is physical and logical user access to audit logs restricted to authorized personnel?	Yes			
		IVS-01.3		Can you provide evidence that due diligence mapping of regulations and standards to your controls/architecture/processes has been done?	Yes			
		IVS-01.4		Are audit logs centrally stored and retained?	Yes			
		IVS-01.5		Are audit logs reviewed on a regular basis for security events (e.g., with automated tools)?	Yes			
Infrastructure & Virtualization Security *Change Detection*	IVS-02	IVS-02.1	**The provider shall ensure the integrity of all virtual machine images at all times. Any changes made to virtual machine images must be logged and an alert raised regardless of their running state (e.g. dormant, off, or running). The results of a change or move of an image and the subsequent validation of the image's integrity must be immediately available to customers through electronic methods (e.g. portals or alerts).**	Do you log and alert any changes made to virtual machine images regardless of their running state (e.g. dormant, off or running)?	Yes			Logged where applicable
		IVS-02.2		Are changes made to virtual machines, or moving of an image and subsequent validation of the image's integrity, made immediately available to customers through electronic methods (e.g. portals or alerts)?			N/A	Adallom is not a IaaS provider

Infrastructure & Virtualization Security *Clock Synchronization*	IVS-03	IVS-03.1	**A reliable and mutually agreed upon external time source shall be used to synchronize the system clocks of all relevant information processing systems to facilitate tracing and reconstitution of activity timelines.**	Do you use a synchronized time-service protocol (e.g., NTP) to ensure all systems have a common time reference?	Yes			
Infrastructure & Virtualization Security *Capacity / Resource Planning*	IVS-04	IVS-04.1	**The availability, quality, and adequate capacity and resources shall be planned, prepared, and measured to deliver the required system performance in accordance with legal, statutory, and regulatory compliance obligations. Projections of future capacity requirements shall be made to mitigate the risk of system overload.**	Do you provide documentation regarding what levels of system (network, storage, memory, I/O, etc.) oversubscription you maintain and under what circumstances/scenarios?		No		
		IVS-04.2		Do you restrict use of the memory oversubscription capabilities present in the hypervisor?			N/A	Adallom is not a IaaS provider
		IVS-04.3		Do your system capacity requirements take into account current, projected and anticipated capacity needs for all systems used to provide services to the tenants?	Yes			
		IVS-04.4		Is system performance monitored and tuned in order to continuously meet regulatory, contractual and business requirements for all the systems used to provide services to the tenants?	Yes			
Infrastructure & Virtualization Security *Management - Vulnerability Management*	IVS-05	IVS-05.1	**Implementers shall ensure that the security vulnerability assessment tools or services accommodate the virtualization technologies used (e.g. virtualization aware).**	Do security vulnerability assessment tools or services accommodate the virtualization technologies being used (e.g. virtualization aware)?			N/A	Adallom is not a IaaS provider
Infrastructure & Virtualization Security *Network Security*	IVS-06	IVS-06.1	**Network environments and virtual instances shall be designed and configured to restrict and monitor traffic between trusted and untrusted connections, these configurations shall be reviewed at least annually, and supported by a documented justification for use for all allowed services, protocols, and ports, and compensating controls.**	For your IaaS offering, do you provide customers with guidance on how to create a layered security architecture equivalence using your virtualized solution?			N/A	Adallom is not a IaaS provider
		IVS-06.2		Do you regularly update network architecture diagrams that include data flows between security domains/zones?	Yes			
		IVS-06.3		Do you regularly review for appropriateness the allowed access/connectivity (e.g., firewall rules) between security domains/zones within the network?	Yes			
		IVS-06.4		Are all firewall access control lists documented with business justification?	Yes			
Infrastructure & Virtualization Security *OS Hardening and Base Controls*	IVS-07	IVS-07.1	**Each operating system shall be hardened to provide only necessary ports, protocols, and services to meet business needs and have in place supporting technical controls such as: antivirus, file integrity monitoring, and logging as part of their baseline operating build standard or template.**	Are operating systems hardened to provide only the necessary ports, protocols and services to meet business needs using technical controls (i.e. antivirus, file integrity monitoring and logging) as part of their baseline build standard or template?	Yes			
Infrastructure & Virtualization Security *Production /*	IVS-08	IVS-08.1	**Production and non-production environments shall be separated to prevent unauthorized access or changes to information assets. Separation of the environments may include: stateful inspection**	For your SaaS or PaaS offering, do you provide tenants with separate environments for production and test processes?	Yes			
		IVS-08.2		For your IaaS offering, do you provide tenants with guidance on how to create suitable production and test environments?			N/A	Adallom is not a IaaS provider

Nonproduction Environments		IVS-08.3	**firewalls, domain/realm authentication sources, and clear segregation of duties for personnel accessing these environments as part of their job duties.**	Do you logically and physically segregate production and non-production environments?	Yes			
Infrastructure & Virtualization Security *Segmentation*	IVS-09	IVS-09.1	**Multi-tenant organizationally-owned or managed (physical and virtual) applications, and infrastructure system and network components, shall be designed, developed, deployed and configured such that provider and customer (tenant) user access is appropriately segmented from other tenant users, based on the following considerations:** **• Established policies and procedures** **• Isolation of business critical assets and/or sensitive user data and sessions that mandate stronger internal controls and high levels of assurance** **• Compliance with legal, statutory and regulatory compliance obligations**	Are system and network environments protected by a firewall or virtual firewall to ensure business and customer security requirements?	Yes			
		IVS-09.2		Are system and network environments protected by a firewall or virtual firewall to ensure compliance with legislative, regulatory and contractual requirements?	Yes			
		IVS-09.3		Are system and network environments protected by a firewall or virtual firewall to ensure separation of production and non-production environments?	Yes			
		IVS-09.4		Are system and network environments protected by a firewall or virtual firewall to ensure protection and isolation of sensitive data?	Yes			
Infrastructure & Virtualization Security *VM Security - vMotion Data Protection*	IVS-10	IVS-10.1	**Secured and encrypted communication channels shall be used when migrating physical servers, applications, or data to virtualized servers and, where possible, shall use a network segregated from production-level networks for such migrations.**	Are secured and encrypted communication channels used when migrating physical servers, applications or data to virtual servers?			N/A	
		IVS-10.2		Do you use a network segregated from production-level networks when migrating physical servers, applications or data to virtual servers?			N/A	
Infrastructure & Virtualization Security *VMM Security - Hypervisor Hardening*	IVS-11	IVS-11.1	**Access to all hypervisor management functions or administrative consoles for systems hosting virtualized systems shall be restricted to personnel based upon the principle of least privilege and supported through technical controls (e.g., two-factor authentication, audit trails, IP address filtering, firewalls, and TLS encapsulated communications to the administrative consoles).**	Do you restrict personnel access to all hypervisor management functions or administrative consoles for systems hosting virtualized systems based on the principle of least privilege and supported through technical controls (e.g. two-factor authentication, audit trails, IP address filtering, firewalls and TLS-encapsulated communications to the administrative consoles)?	Yes			Enforced where applicable
Infrastructure & Virtualization Security *Wireless Security*	IVS-12	IVS-12.1	**Policies and procedures shall be established, and supporting business processes and technical measures implemented, to protect wireless network environments, including the following:** **• Perimeter firewalls implemented and configured to restrict unauthorized traffic** **• Security settings enabled with strong encryption for authentication and transmission, replacing**	Are policies and procedures established and mechanisms configured and implemented to protect the wireless network environment perimeter and to restrict unauthorized wireless traffic?	Yes			
		IVS-12.2		Are policies and procedures established and mechanisms implemented to ensure wireless security settings are enabled with strong encryption for authentication and transmission, replacing vendor default settings? (e.g., encryption keys, passwords, SNMP community strings)	Yes			

		IVS-12.3	**vendor default settings (e.g., encryption keys, passwords, and SNMP community strings)** **• User access to wireless network devices restricted to authorized personnel** **• The capability to detect the presence of unauthorized (rogue) wireless network devices for a timely disconnect from the network**	Are policies and procedures established and mechanisms implemented to protect wireless network environments and detect the presence of unauthorized (rogue) network devices for a timely disconnect from the network?			N/A	Wireless network provides public access only. Sensitive content requires access to internal networks not available through wireless
Infrastructure & Virtualization Security *Network Architecture*	IVS-13	IVS-13.1	**Network architecture diagrams shall clearly identify high-risk environments and data flows that may have legal compliance impacts. Technical measures shall be implemented and shall apply defense-in-depth techniques (e.g., deep packet analysis, traffic throttling, and black-holing) for detection and timely response to network-based attacks associated with anomalous ingress or egress traffic patterns (e.g., MAC spoofing and ARP poisoning attacks) and/or distributed denial-of-service (DDoS) attacks.**	Do your network architecture diagrams clearly identify high-risk environments and data flows that may have legal compliance impacts?	Yes			
		IVS-13.2		Do you implement technical measures and apply defense-in-depth techniques (e.g., deep packet analysis, traffic throttling and black-holing) for detection and timely response to network-based attacks associated with anomalous ingress or egress traffic patterns (e.g., MAC spoofing and ARP poisoning attacks) and/or distributed denial-of-service (DDoS) attacks?	Yes			
Interoperability & Portability *APIs*	IPY-01	IPY-01	**The provider shall use open and published APIs to ensure support for interoperability between components and to facilitate migrating applications.**	Do you publish a list of all APIs available in the service and indicate which are standard and which are customized?	Yes			
Interoperability & Portability *Data Request*	IPY-02	IPY-02	**All structured and unstructured data shall be available to the customer and provided to them upon request in an industry-standard format (e.g., .doc, .xls, .pdf, logs, and flat files)**	Is unstructured customer data available on request in an industry-standard format (e.g., .doc, .xls, or .pdf)?	Yes			
Interoperability & Portability *Policy & Legal*	IPY-03	IPY-03.1	**Policies, procedures, and mutually-agreed upon provisions and/or terms shall be established to satisfy customer (tenant) requirements for service-to-service application (API) and information processing interoperability, and portability for application development and information exchange, usage and integrity persistence.**	Do you provide policies and procedures (i.e. service level agreements) governing the use of APIs for interoperability between your service and third-party applications?	Yes			
		IPY-03.2		Do you provide policies and procedures (i.e. service level agreements) governing the migration of application data to and from your service?	Yes			
Interoperability & Portability *Standardized Network Protocols*	IPY-04	IPY-04.1	**The provider shall use secure (e.g., non-clear text and authenticated) standardized network protocols for the import and export of data and to manage the service, and shall make available a document to consumers (tenants) detailing the relevant interoperability and portability standards that are involved.**	Can data import, data export and service management be conducted over secure (e.g., non-clear text and authenticated), industry accepted standardized network protocols?	Yes			
		IPY-04.2		Do you provide consumers (tenants) with documentation detailing the relevant interoperability and portability network protocol standards that are involved?	Yes			
Interoperability & Portability	IPY-05	IPY-05.1	**The provider shall use an industry-recognized virtualization platform and standard virtualization**	Do you use an industry-recognized virtualization platform and standard virtualization formats (e,g., OVF) to help ensure interoperability?			N/A	Adallom is not an IaaS provider

Virtualization		IPY-05.2	**formats (e.g., OVF) to help ensure interoperability, and shall have documented custom changes made to any hypervisor in use, and all solution-specific virtualization hooks, available for customer review.**	Do you have documented custom changes made to any hypervisor in use, and all solution-specific virtualization hooks available for customer review?			N/A	Adallom is not an IaaS provider
Mobile Security *Anti-Malware*	MOS-01	MOS-01	**Anti-malware awareness training, specific to mobile devices, shall be included in the provider's information security awareness training.**	Do you provide anti-malware training specific to mobile devices as part of your information security awareness training?		No		
Mobile Security *Application Stores*	MOS-02	MOS-02	**A documented list of approved application stores has been communicated as acceptable for mobile devices accessing or storing provider managed data.**	Do you document and make available lists of approved application stores for mobile devices accessing or storing company data and/or company systems?		No		Adallom does not white listing applications for employee devices
Mobile Security *Approved Applications*	MOS-03	MOS-03	**The company shall have a documented policy prohibiting the installation of non-approved applications or approved applications not obtained through a pre-identified application store.**	Do you have a policy enforcement capability (e.g., XACML) to ensure that only approved applications and those from approved application stores be loaded onto a mobile device?	Yes			Adallom can be used to enforce access policies to mobile devices
Mobile Security *Approved Software for BYOD*	MOS-04	MOS-04	**The BYOD policy and supporting awareness training clearly states the approved applications, application stores, and application extensions and plugins that may be used for BYOD usage.**	Does your BYOD policy and training clearly state which applications and applications stores are approved for use on BYOD devices?		No		Adallom does not white listing applications for employee devices
Mobile Security *Awareness and Training*	MOS-05	MOS-05	**The provider shall have a documented mobile device policy that includes a documented definition for mobile devices and the acceptable usage and requirements for all mobile devices. The provider shall post and communicate the policy and requirements through the company's security awareness and training program.**	Do you have a documented mobile device policy in your employee training that clearly defines mobile devices and the accepted usage and requirements for mobile devices?	Yes			
Mobile Security *Cloud Based Services*	MOS-06	MOS-06	**All cloud-based services used by the company's mobile devices or BYOD shall be pre-approved for usage and the storage of company business data.**	Do you have a documented list of pre-approved cloud based services that are allowed to be used for use and storage of company business data via a mobile device?	Yes			
Mobile Security *Compatibility*	MOS-07	MOS-07	**The company shall have a documented application validation process to test for mobile device, operating system, and application compatibility issues.**	Do you have a documented application validation process for testing device, operating system and application compatibility issues?		No		
Mobile Security *Device Eligibility*	MOS-08	MOS-08	**The BYOD policy shall define the device and eligibility requirements to allow for BYOD usage.**	Do you have a BYOD policy that defines the device(s) and eligibility requirements allowed for BYOD usage?	Yes			
Mobile Security *Device Inventory*	MOS-09	MOS-09	**An inventory of all mobile devices used to store and access company data shall be kept and maintained. All changes to the status of these devices, (i.e., operating system and patch levels, lost or decommissioned status, and to whom the device is assigned or approved for usage (BYOD), will be included for each device in the inventory.**	Do you maintain an inventory of all mobile devices storing and accessing company data which includes device status (os system and patch levels, lost or decommissioned, device assignee)?	Yes			

Mobile Security *Device Management*	MOS-10	MOS-10	**A centralized, mobile device management solution shall be deployed to all mobile devices permitted to store, transmit, or process customer data.**	Do you have a centralized mobile device management solution deployed to all mobile devices that are permitted to store, transmit, or process company data?	Yes			
Mobile Security *Encryption*	MOS-11	MOS-11	**The mobile device policy shall require the use of encryption either for the entire device or for data identified as sensitive on all mobile devices and shall be enforced through technology controls.**	Does your mobile device policy require the use of encryption for either the entire device or for data identified as sensitive enforceable through technology controls for all mobile devices?	Yes			
Mobile Security *Jailbreaking and Rooting*	MOS-12	MOS-12.1	**The mobile device policy shall prohibit the circumvention of built-in security controls on mobile devices (e.g. jailbreaking or rooting) and isenforced through detective and preventative controls on the device or through a centralized device management system (e.g. mobile device management).**	Does your mobile device policy prohibit the circumvention of built-in security controls on mobile devices (e.g., jailbreaking or rooting)?	Yes			
		MOS-12.2		Do you have detective and preventative controls on the device or via a centralized device management system which prohibit the circumvention of built-in security controls?	Yes			
Mobile Security *Legal*	MOS-13	MOS-13.1	**The BYOD policy includes clarifying language for the expectation of privacy, requirements for litigation, e-discovery, and legal holds. The BYOD policy shall clearly state the expectations over the loss of non-company data in the case a wipe of the device is required.**	Does your BYOD policy clearly define the expectation of privacy, requirements for litigation, e-discovery and legal holds?	Yes			
		MOS-13.2		Do you have detective and preventative controls on the device or via a centralized device management system which prohibit the circumvention of built-in security controls?		No		
Mobile Security *Lockout Screen*	MOS-14	MOS-14	**BYOD and/or company owned devices are configured to require an automatic lockout screen, and the requirement shall be enforced through technical controls.**	Do you require and enforce via technical controls an automatic lockout screen for BYOD and company owned devices?	Yes			
Mobile Security *Operating Systems*	MOS-15	MOS-15	**Changes to mobile device operating systems, patch levels, and/or applications shall be managed through the company's change management processes.**	Do you manage all changes to mobile device operating systems, patch levels and applications via your company's change management processes?		No		
Mobile Security *Passwords*	MOS-16	MOS-16.1	**Password policies, applicable to mobile devices, shall be documented and enforced through technical controls on all company devices or devices approved for BYOD usage, and shall prohibit the changing of password/PIN lengths and authentication requirements.**	Do you have password policies for enterprise issued mobile devices and/or BYOD mobile devices?	Yes			
		MOS-16.2		Are your password policies enforced through technical controls (i.e. MDM)?		No		
		MOS-16.3		Do your password policies prohibit the changing of authentication requirements (i.e. password/PIN length) via a mobile device?		No		
Mobile Security *Policy*	MOS-17	MOS-17.1	**The mobile device policy shall require the BYOD user to perform backups of data, prohibit the usage of unapproved application stores, and require the use of anti-malware software (where supported).**	Do you have a policy that requires BYOD users to perform backups of specified corporate data?	Yes			
		MOS-17.2		Do you have a policy that requires BYOD users to prohibit the usage of unapproved application stores?	Yes			
		MOS-17.3		Do you have a policy that requires BYOD users to use anti-malware software (where supported)?	Yes			
Mobile Security *Remote Wipe*	MOS-18	MOS-18.1	**All mobile devices permitted for use through the company BYOD program or a company-assigned**	Does your IT provide remote wipe or corporate data wipe for all company-accepted BYOD devices?	Yes			

		MOS-18.2	**mobile device shall allow for remote wipe by the company's corporate IT or shall have all company-provided data wiped by the company's corporate IT.**	Does your IT provide remote wipe or corporate data wipe for all company-assigned mobile devices?	Yes			
Mobile Security *Security Patches*	MOS-19	MOS-19.1	**Mobile devices connecting to corporate networks or storing and accessing company information shall allow for remote software version/patch validation. All mobile devices shall have the latest available security-related patches installed upon general release by the device manufacturer or carrier and authorized IT personnel shall be able to perform these updates remotely.**	Do your mobile devices have the latest available security-related patches installed upon general release by the device manufacturer or carrier?	Yes			
		MOS-19.2		Do your mobile devices allow for remote validation to download the latest security patches by company IT personnel?		No		
Mobile Security *Users*	MOS-20	MOS-20.1	**The BYOD policy shall clarify the systems and servers allowed for use or access on a BYOD-enabled device.**	Does your BYOD policy clarify the systems and servers allowed for use or access on the BYOD-enabled device?	Yes			
		MOS-20.2		Does your BYOD policy specify the user roles that are allowed access via a BYOD-enabled device?	Yes			
Security Incident Management, E-Discovery & Cloud Forensics *Contact / Authority Maintenance*	SEF-01	SEF-01.1	**Points of contact for applicable regulation authorities, national and local law enforcement, and other legal jurisdictional authorities shall be maintained and regularly updated (e.g., change in impacted-scope and/or a change in any compliance obligation) to ensure direct compliance liaisons have been established and to be prepared for a forensic investigation requiring rapid engagement with law enforcement.**	Do you maintain liaisons and points of contact with local authorities in accordance with contracts and appropriate regulations?	Yes			
Security Incident Management, E-Discovery & Cloud Forensics *Incident Management*	SEF-02	SEF-02.1	**Policies and procedures shall be established, and supporting business processes and technical measures implemented, to triage security-related events and ensure timely and thorough incident management, as per established IT service management policies and procedures.**	Do you have a documented security incident response plan?	Yes			
		SEF-02.2		Do you integrate customized tenant requirements into your security incident response plans?	Yes			
		SEF-02.3		Do you publish a roles and responsibilities document specifying what you vs. your tenants are responsible for during security incidents?	Yes			Available upon request
		SEF-02.4		Have you tested your security incident response plans in the last year?	Yes			
Security Incident Management, E-Discovery & Cloud Forensics *Incident Reporting*	SEF-03	SEF-03.1	**Workforce personnel and external business relationships shall be informed of their responsibility and, if required, shall consent and/or contractually agree to report all information security events in a timely manner. Information security events shall be reported through predefined communications channels in a timely manner adhering to applicable legal, statutory, or regulatory compliance obligations.**	Does your security information and event management (SIEM) system merge data sources (app logs, firewall logs, IDS logs, physical access logs, etc.) for granular analysis and alerting?	Yes			
		SEF-03.2		Does your logging and monitoring framework allow isolation of an incident to specific tenants?	Yes			
Security Incident Management, E-Discovery &	SEF-04	SEF-04.1	**Proper forensic procedures, including chain of custody, are required for the presentation of evidence to support potential legal action subject to**	Does your incident response plan comply with industry standards for legally admissible chain-of-custody management processes and controls?	Yes			
		SEF-04.2		Does your incident response capability include the use of legally admissible forensic data	Yes			

Cloud Forensics *Incident Response Legal Preparation*			**the relevant jurisdiction after an information security incident. Upon notification, customers and/or other external business partners impacted by a security breach shall be given the opportunity to participate as is legally permissible in the forensic investigation.**	collection and analysis techniques?				
		SEF-04.3		Are you capable of supporting litigation holds (freeze of data from a specific point in time) for a specific tenant without freezing other tenant data?	Yes			
		SEF-04.4		Do you enforce and attest to tenant data separation when producing data in response to legal subpoenas?	Yes			
Security Incident Management, E-Discovery & Cloud Forensics *Incident Response Metrics*	SEF-05	SEF-05.1	**Mechanisms shall be put in place to monitor and quantify the types, volumes, and costs of information security incidents.**	Do you monitor and quantify the types, volumes and impacts on all information security incidents?	Yes			
		SEF-05.2		Will you share statistical information for security incident data with your tenants upon request?	Yes			
Supply Chain Management, Transparency and Accountability *Data Quality and Integrity*	STA-01	STA-01.1	**Providers shall inspect, account for, and work with their cloud supply-chain partners to correct data quality errors and associated risks. Providers shall design and implement controls to mitigate and contain data security risks through proper separation of duties, role-based access, and least-privilege access for all personnel within their supply chain.**	Do you inspect and account for data quality errors and associated risks, and work with your cloud supply-chain partners to correct them?	Yes			
		STA-01.2		Do you design and implement controls to mitigate and contain data security risks through proper separation of duties, role-based access, and least-privileged access for all personnel within your supply chain?	Yes			
Supply Chain Management, Transparency and Accountability *Incident Reporting*	STA-02	STA-02.1	**The provider shall make security incident information available to all affected customers and providers periodically through electronic methods (e.g. portals).**	Do you make security incident information available to all affected customers and providers periodically through electronic methods (e.g. portals)?	Yes			
Supply Chain Management, Transparency and Accountability *Network / Infrastructure Services*	STA-03	STA-03.1	**Business-critical or customer (tenant) impacting (physical and virtual) application and system-system interface (API) designs and configurations, and infrastructure network and systems components, shall be designed, developed, and deployed in accordance with mutually agreed-upon service and capacity-level expectations, as well as IT governance and service management policies and procedures.**	Do you collect capacity and use data for all relevant components of your cloud service offering?	Yes			
		STA-03.2		Do you provide tenants with capacity planning and use reports?		No		
Supply Chain Management, Transparency and Accountability *Provider Internal Assessments*	STA-04	STA-04.1	**The provider shall perform annual internal assessments of conformance and effectiveness of its policies, procedures, and supporting measures and metrics.**	Do you perform annual internal assessments of conformance and effectiveness of your policies, procedures, and supporting measures and metrics?	Yes			

Supply Chain Management, Transparency and Accountability *Third Party Agreements*	STA-05	STA-05.1	**Supply chain agreements (e.g., SLAs) between providers and customers (tenants) shall incorporate at least the following mutually-agreed upon provisions and/or terms […]**	Do you select and monitor outsourced providers in compliance with laws in the country where the data is processed, stored and transmitted?	Yes			
		STA-05.2		Do you select and monitor outsourced providers in compliance with laws in the country where the data originates?	Yes			
		STA-05.3		Does legal counsel review all third-party agreements?	Yes			
		STA-05.4		Do third-party agreements include provision for the security and protection of information and assets?	Yes			
		STA-05.5		Do you provide the client with a list and copies of all subprocessing agreements and keep this updated?		No		
Supply Chain Management, Transparency and Accountability *Supply Chain Governance Reviews*	STA-06	STA-06.1	**Providers shall review the risk management and governance processes of their partners so that practices are consistent and aligned to account for risks inherited from other members of that partner's cloud supply chain.**	Do you review the risk management and governanced processes of partners to account for risks inherited from other members of that partner's supply chain?	Yes			
Supply Chain Management, Transparency and Accountability *Supply Chain Metrics*	STA-07	STA-07.1	**Policies and procedures shall be implemented to ensure the consistent review of service agreements (e.g., SLAs) between providers and customers (tenants) across the relevant supply chain (upstream/downstream).** **Reviews shall performed at least annually and identity non-conformance to established agreements. The reviews should result in actions to address service-level conflicts or inconsistencies resulting from disparate supplier relationships.**	Are policies and procedures established, and supporting business processes and technical measures implemented, for maintaining complete, accurate and relevant agreements (e.g., SLAs) between providers and customers (tenants)?	Yes			
		STA-07.2		Do you have the ability to measure and address non-conformance of provisions and/or terms across the entire supply chain (upstream/downstream)?	Yes			
		STA-07.3		Can you manage service-level conflicts or inconsistencies resulting from disparate supplier relationships?	Yes			
		STA-07.4		Do you review all agreements, policies and processes at least annually?	Yes			Performed as part of the annual SOC 2 review
Supply Chain Management, Transparency and Accountability *Third Party Assessment*	STA-08	STA-08.1	**Providers shall assure reasonable information security across their information supply chain by performing an annual review. The review shall include all partners/third party providers upon which their information supply chain depends on.**	Do you assure reasonable information security across your information supply chain by performing an annual review?	Yes			
		STA-08.2		Does your annual review include all partners/third-party providers upon which your information supply chain depends?	Yes			
Supply Chain Management, Transparency	STA-09	STA-09.1	**Third-party service providers shall demonstrate compliance with information security and confidentiality, access control, service definitions,**	Do you permit tenants to perform independent vulnerability assessments?	Yes			

and Accountability *Third Party Audits*		STA-09.2	**and delivery level agreements included in third-party contracts. Third-party reports, records, and services shall undergo audit and review at least annually to govern and maintain compliance with the service delivery agreements.**	Do you have external third party services conduct vulnerability scans and periodic penetration tests on your applications and networks?	Yes			
Threat and Vulnerbility Management *Antivirus / Malicious Software*	TVM-01	TVM-01.1	**Policies and procedures shall be established, and supporting business processes and technical measures implemented, to prevent the execution of malware on organizationally-owned or managed user end-point devices (i.e., issued workstations, laptops, and mobile devices) and IT infrastructure network and systems components.**	Do you have anti-malware programs that support or connect to your cloud service offerings installed on all of your systems?	Yes			
		TVM-01.2		Do you ensure that security threat detection systems using signatures, lists or behavioural patterns are updated across all infrastructure components within industry accepted time frames?	Yes			
Threat and Vulnerbility Management *Vulnerability / Patch Management*	TVM-02	TVM-02.1	**Policies and procedures shall be established, and supporting processes and technical measures implemented, for timely detection of vulnerabilities within organizationally-owned or managed applications, infrastructure network and system components (e.g. network vulnerability assessment, penetration testing) to ensure the efficiency of implemented security controls. A risk-based model for prioritizing remediation of identified vulnerabilities shall be used. Changes shall be managed through a change management process for all vendor-supplied patches, configuration changes, or changes to the organization's internally developed software. Upon request, the provider informs customer (tenant) of policies and procedures and identified weaknesses especially if customer (tenant) data is used as part the service and/or customer (tenant) has some shared responsibility over implementation of control.**	Do you conduct network-layer vulnerability scans regularly as prescribed by industry best practices?	Yes			
		TVM-02.2		Do you conduct application-layer vulnerability scans regularly as prescribed by industry best practices?	Yes			
		TVM-02.3		Do you conduct local operating system-layer vulnerability scans regularly as prescribed by industry best practices?	Yes			
		TVM-02.4		Will you make the results of vulnerability scans available to tenants at their request?	Yes			
		TVM-02.5		Do you have a capability to rapidly patch vulnerabilities across all of your computing devices, applications and systems?	Yes			
		TVM-02.6		Will you provide your risk-based systems patching time frames to your tenants upon request?	Yes			
Threat and Vulnerbility Management *Mobile Code*	TVM-03	TVM-03.1	**Policies and procedures shall be established, and supporting business processes and technical measures implemented, to prevent the execution of unauthorized mobile code, defined as software**	Is mobile code authorized before its installation and use, and the code configuration checked, to ensure that the authorized mobile code operates according to a clearly defined security policy?	Yes			

		TVM-03.2	**transferred between systems over a trusted or untrusted network and executed on a local system without explicit installation or execution by the recipient, on organizationally-owned or managed user end-point devices (e.g., issued workstations, laptops, and mobile devices) and IT infrastructure network and systems components.**	Is all unauthorized mobile code prevented from executing?	Yes				

Tabla 23. CAI Questionnaire v3.0.1. Controles.

Anexo C: CAIQ (II). Estándares

A continuación se muestra el extracto del CAIQ correspondiente a la información de los estándares asociados a los *Control Groups*. Debido al tamaño de la tabla se muestra para un *Control Group* específico, *Application & Interface Security – Application Security*. Además, se encuentra divida en tres tablas, en cada una de las cuales se muestra un conjunto de los estándares incluidos en el CAIQ.

Control Group	CGID	CID	CCM v3.0.1 Compliance Mapping										
			AICPA TSC 2009	AICPA Trust Service Criteria (SOC 2SM Report)	AICPA TSC 2014	BITS Shared Assessments AUP v5.0	BITS Shared Assessments SIG v6.0	BSI Germany	Canada PIPEDA	CCM V1.X	COBIT 4.1	COBIT 5.0	COPPA
Application & Interface Security *Application Security*	AIS-01	AIS-01.1	S3.10.0	(S3.10.0) Design, acquisition, implementation, configuration, modification, and management of infrastructure and software are consistent with defined system security policies to enable authorized access and to prevent unauthorized access. (S3.10.0) Design, acquisition, implementation, configuration, modification, and management of infrastructure and software are consistent with defined processing integrity and related security policies.	CC7.1	I.4	G.16.3, I.3		Schedule 1 (Section 5), 4.7 - Safeguards, Subsec. 4.7.3	SA-04	COBIT 4.1 AI2.4	APO09.03 APO13.01 BAI03.01 BAI03.02 BAI03.03 BAI03.05 MEA03.01 MEA03.02	312.8 and 312.10
		AIS-01.2											
		AIS-01.3											
		AIS-01.4											
		AIS-01.5											

Tabla 24. CAI Questionnaire v3.0.1. Estándares (I).

Control Group	CGID	CID	CCM v3.0.1 Compliance Mapping											
			CSA Enterprise Architecture (formerly the Trusted Cloud Initiative)			CSA Guidance V3.0	ENISA IAF	95/46/EC - European Union Data Protection Directive	FedRAMP Security Controls (Final Release, Jan 2012) --LOW IMPACT LEVEL--	FedRAMP Security Controls (Final Release, Jan 2012) --MODERATE IMPACT LEVEL--	FERPA	GAPP (Aug 2009)	HIPAA/HITECH (Omnibus Rule)
			Domain > Container > Capability	Public	Private								
Application & Interface Security *Application Security*	AIS-01	AIS-01.1 AIS-01.2 AIS-01.3 AIS-01.4 AIS-01.5	Application Services > Development Process > Software Quality Assurance	shared	x	Domain 10	6.03.01. (c)	Article: 27 (3)	NIST SP 800-53 R3 SC-5 NIST SP 800-53 R3 SC-6 NIST SP 800-53 R3 SC-7 NIST SP 800-53 R3 SC-12 NIST SP 800-53 R3 SC-13 NIST SP 800-53 R3 SC-14	NIST SP 800-53 R3 SA-8, NIST SP 800-53 R3 SC-2, NIST SP 800-53 R3 SC-4, NIST SP 800-53 R3 SC-5, NIST SP 800-53 R3 SC-6, NIST SP 800-53 R3 SC-7, NIST SP 800-53 R3 SC-7 (1), NIST SP 800-53 R3 SC-7 (2), NIST SP 800-53 R3 SC-7 (3), NIST SP 800-53 R3 SC-7 (4), NIST SP 800-53 R3 SC-7 (5), NIST SP 800-53 R3 SC-7 (7), NIST SP 800-53 R3 SC-7 (8), NIST SP 800-53 R3 SC-7 (12), NIST SP 800-53 R3 SC-7 (13), NIST SP 800-53 R3 SC-7 (18), NIST SP 800-53 R3 SC-8, NIST SP 800-53 R3 SC-8 (1), NIST SP 800-53 R3 SC-9, NIST SP 800-53 R3 SC-9 (1), NIST SP 800-53 R3 SC-10, NIST SP 800-53 R3 SC-11, NIST SP 800-53 R3 SC-12 NIST SP 800-53 R3 SC-12 (2), NIST SP 800-53 R3 SC-12 (5), NIST SP 800-53 R3 SC-13, NIST SP 800-53 R3 SC-13 (1), NIST SP 800-53 R3 SC-14, NIST SP 800-53 R3 SC-17, NIST SP 800-53 R3 SC-18		1.2.6	45 CFR 164.312(e)(2)(i)

Tabla 25. CAI Questionnaire v3.0.1. Estándares (II).

Control Group	CGID	CID	CCM v3.0.1 Compliance Mapping												
			ISO/IEC 27001:2005	ISO/IEC 27001:2013	ITAR	Jericho Forum	Mexico - Federal Law on Protection of Personal Data Held by Private Parties	NERC CIP	NIST SP800-53 R3	NIST SP800-53 R4 Appendix J	NZISM	ODCA UM: PA R2.0		PCI DSS v2.0	PCI DSS v3.0
												PA ID	PA level		
Application & Interface Security *Application Security*	AIS-01	AIS-01.1 AIS-01.2 AIS-01.3 AIS-01.4 AIS-01.5	A.11.5.6 A.11.6.1 A.12.2.1 A.12.2.2 A.12.2.3 A.12.2.4 A.12.5.2 A.12.5.4 A.12.5.5 A.12.6.1 A.15.2.1	A9.4.2 A9.4.1, 8.1*Partial, A14.2.3, 8.1*partial, A.14.2.7 A12.6.1, A18.2.2		Commandment #1 Commandment #2 Commandment #4 Commandment #5 Commandment #11		CIP-007-3 - R5.1	SC-2 SC-3 SC-4 SC-5 SC-6 SC-7 SC-8 SC-9 SC-10 SC-11 SC-12 SC-13 SC-14 SC-17 SC-18 SC-20 SC-21 SC-22 SC-23	AR-7 The organization designs information systems to support privacy by automating privacy controls.	14.5 14.6	PA17 PA31	SGP BSGP	PCI DSS v2.0 6.5	6, 6.5

Tabla 26. CAI Questionnaire v3.0.1. Estándares (III).